BIG-IP® Local Traffic Manager: Implementations

バージョン 10.0.0

MAN-0293-00

製品バージョン

本マニュアルは、BIG-IP 製品ファミリのバージョン 10.0.0 に適用されます。

利用規約

著作権

Copyright 2009, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc.（F5）では、本マニュアルに記載されている情報を正確かつ信頼性のあるものであると考えています。ただし、F5 は、この情報の使用、あるいはこの情報の使用から生じる第三者の特許または他の権利の侵害に関していかなる責任も負いません。該当するユーザライセンスにより明確に規定される場合を除き、F5 のすべての特許権、著作権、その他の知的財産権の下、明示的または暗黙的なライセンスを一切付与しません。F5 は、予告なしにいかなる時点でも仕様を変更する権利を保有します。

商標

F5、F5 Networks、F5 のロゴ、BIG-IP、3-DNS、Acopia、Acopia Networks、Application Accelerator、Ask F5、Application Security Manager、ASM、ARX、Data Guard、Enterprise Manager、EM、FirePass、FreedomFabric、Global Traffic Manager、GTM、iControl、Intelligent Browser Referencing、Internet Control Architecture、IP Application Switch、iRules、Link Controller、LC、Local Traffic Manager、LTM、Message Security Module、MSM、NetCelera、OneConnect、Packet Velocity、SSL Accelerator、SYN Check、Traffic Management Operating System、TMOS、TrafficShield、Transparent Data Reduction、uRoam、VIPRION、WANJet、WebAccelerator、および ZoneRunner は、米国および他の国における F5 Networks, Inc. の商標または登録商標で、F5 から明示的な書面による同意を受けていない使用は禁止されています。

特許権

本製品は米国特許番号 6,374,300; 6,473,802; 6,970,933; 7,051,126; 7,102,996; 7,146,354; 7,197,661; 7,206,282; 7,287,084 で保護されています。そのほかの特許は申請中です。

輸出規制に関する通知

本製品は、暗号化ソフトウェアを含む場合があります。輸出管理法（Export Administration Act）に基づき、本製品の米国外への輸出は、米国政府から違法行為とみなされる可能性があります。

無線周波数妨害に関する警告

本製品は Class A 製品です。米国内の環境では、本製品によって電波障害が発生する可能性があります。その場合は適切な対処策が必要です。

FCC への準拠

本製品は、FCC 規則の第 15 章に定められている Class A デジタルデバイスに関する規制要件に基づいて所定の試験を実施し、その適合性が認定されています。これらの制限は、本製品が商用環境で動作する際の有害な無線周波数妨害に対して適切な保護機能を提供することを目的としています。このユニットは、無線周波数エネルギーを発生および使用し、場合によっては放射する可能性があります。そのため、取扱説明書に従った設置や使用を行わない場合、無線通信に対して有害な妨害を生じることがあります。住宅地域で本製品を使用すると無線周波妨害が発生する可能性があります。その場合、ユーザは妨害状態を回避するために必要な手段を講じる必要があります。

製造元からの明示的な承認を受けずに本製品に変更を加えた場合、FCC 規則の第 15 章に基づいて本製品を操作するユーザの権限が無効になることがあります。

カナダ国内の規定に対する準拠

この Class A デジタル機器は、カナダの ICES-003 に準拠しています。

規格準拠

本製品は、製造時点で、情報テクノロジ製品に適用可能な IEC、European Union、ANSI/UL、および Canadian CSA 標準に準拠しています。

謝辞

本製品には、Bill Paul により開発されたソフトウェアが含まれています。

本製品には、Jonathan Stone により開発されたソフトウェアが含まれています。

本製品には、Manuel Bouyer により開発されたソフトウェアが含まれています。

本製品には、Paul Richards により開発されたソフトウェアが含まれています。

本製品には、NetBSD Foundation, Inc. およびその貢献者により開発されたソフトウェアが含まれています。

本製品には、Politecnico di Torino およびその貢献者により開発されたソフトウェアが含まれています。

本製品には、Swedish Institute of Computer Science およびその貢献者により開発されたソフトウェアが含まれています。

本製品には、University of California, Berkey およびその貢献者により開発されたソフトウェアが含まれています。

本製品には、Lawrence Berkeley Laboratory の Computer System Engineering Group により開発されたソフトウェアが含まれています。

本製品には、NetBSD プロジェクト用に Christopher G. Demetriou により開発されたソフトウェアが含まれています。

本製品には、Adam Glass により開発されたソフトウェアが含まれています。

本製品には、Christian E. Hopps により開発されたソフトウェアが含まれています。

本製品には、Dean Huxley により開発されたソフトウェアが含まれています。

本製品には、John Kohl により開発されたソフトウェアが含まれています。

本製品には、Paul Kranenburg により開発されたソフトウェアが含まれています。

本製品には、Terrence R. Lambert により開発されたソフトウェアが含まれています。

本製品には、Philip A. Nelson により開発されたソフトウェアが含まれています。

本製品には、Herb Peyerl により開発されたソフトウェアが含まれています。

本製品には、NetBSD プロジェクト用に Jochen Pohl により開発されたソフトウェアが含まれています。

本製品には、Chris Provenzano により開発されたソフトウェアが含まれています。

本製品には、Theo de Raadt により開発されたソフトウェアが含まれています。

本製品には、David Muir Sharnoff により開発されたソフトウェアが含まれています。

本製品には、SigmaSoft の Th. Lockert により開発されたソフトウェアが含まれています。

本製品には、NetBSD プロジェクト用に Jason R. Thorpe により開発されたソフトウェアが含まれています。

本製品には、And Communications（http://www.and.com）用に Jason R. Thorpe により開発されたソフトウェアが含まれています。

本製品には、NetBSD プロジェクト用に Frank Van der Linden により開発されたソフトウェアが含まれています。

本製品には、NetBSD プロジェクト用に John M. Vinopal により開発されたソフトウェアが含まれています。

本製品には、Christos Zoulas により開発されたソフトウェアが含まれています。

本製品には、University of Vermont および State Agricultural College と Garrett A. Wollman により開発されたソフトウェアが含まれています。

本製品には、Balazs Scheidler <bazsi@balabit.hu> により開発され、GNU Public License に基づいて保護されているソフトウェアが含まれています。

本製品には、Niels Mueller <nisse@lysator.liu.se> により開発され、GNU Public License に基づいて保護されているソフトウェアが含まれています。

次の文で、「このソフトウェア」とは Mitsumi CD-ROM ドライバを指しています。このソフトウェアは、Holger Veit および Brian Moore によって、「386BSD」および類似のオペレーティングシステム用に開発されました。「同様のオペレーティングシステム」には、「NetBSD」、「FreeBSD」、「Mach」（カーネギーメロン大学（CMU）開発）など、主として非営利の研究、教育用システムが含まれています。

本製品には、Apache Group によって Apache HTTP サーバプロジェクト（http://www.apache.org/）用に開発されたソフトウェアが含まれています。

本製品には、GNU Library General Public License（© 1998, Red Hat Software）（www.gnu.org/copyleft/lgpl.html）の下、Richard H. Porter から使用許諾されたソフトウェアが含まれています。

本製品には、Perl Artistic License（© 1997, 1998 Tom Christiansen and Nathan Torkington）の下で使用許諾された Perl ソフトウェアの標準版が含まれています。All rights reserved. 最新の Perl 標準版は、http://www.perl.com で入手できます。

本製品には、Jared Minch により開発されたソフトウェアが含まれています。

本製品には、OpenSSL Toolkit（http://www.openssl.org/）での使用を目的として、OpenSSL プロジェクトにより開発されたソフトウェアが含まれています。

本製品には、Eric Young（eay@cryptsoft.com）により作成された暗号化ソフトウェアが含まれています。

本製品には、GNU Public License で保護されている oprofile に基づくソフトウェアが含まれています。

本製品には、Tobi Oetiker 氏（http://www.rrdtool.com/index.html）が開発し、GNU General Public License に基づきライセンス付与されている RRDtool が含まれています。

本製品には、GNU General Public License（GPL）の許可を受けて、Dr. Brian Gladman から使用許諾されたソフトウェアが含まれています。

本製品には、Apache Software Foundation <http://www.apache.org/> により開発されたソフトウェアが含まれています。

本製品には、Hypersonic SQL が含まれています。

本製品にはカリフォルニア大学の指導教授、Sun Microsystems, Inc.、Scriptics Corporation、その他の企業等が共同開発したソフトウェアが含まれています。

本製品には、Internet Software Consortium により開発されたソフトウェアが含まれています。

本製品には、Nominum, Inc.（http://www.nominum.com）により開発されたソフトウェアが含まれています。

この製品には Broadcom Corporation が開発し、GNU Public License に基づき保護されているソフトウェアが含まれています。

目次

1
BIG-IP LTM の実装の概要

BIG-IP 実装の概要 1-1
はじめに 1-1
設定ユーティリティの使用 1-1
本ガイドについて 1-2
補足情報 1-2
表記規則 1-3
ヘルプおよびテクニカルサポートリソースへのアクセス 1-5

2
nPath ルーティングの設定

nPath ルーティングの概要 2-1
nPath ルーティングの設定 2-2
カスタムの Fast L4 プロファイルの作成 2-3
nPath ルーティング用のサーバプールの作成 2-4
バーチャルサーバの作成 2-4
コンテンツサーバのループバックインターフェイスでのバーチャルサーバアドレスの設定 2-5
着信トラフィック用ルートの設定 2-5
connection.autolasthop bigdb キーの有効化 2-5
nPath 設定用のタイマの設定 2-6
UDP トラフィックでのタイムアウトの設定ガイドライン 2-6
TCP トラフィックでのタイムアウトの設定ガイドライン 2-6

3
Web サイトおよび電子商取引の基本設定

Web サイトおよび電子商取引の基本設定での作業 3-1
基本的な電子商取引サイトの設定 3-2
ロードバランシングプールの作成 3-2
バーチャルサーバの作成 3-3

4
IP ネットワークを変更しない BIG-IP のインストール

IP ネットワークを変更しない BIG-IP のインストール 4-1
同じ IP ネットワークの BIG-IP の設定 4-3
個々の VLAN からのセルフ IP アドレスの削除 4-3
VLAN グループの作成 4-4
VLAN グループ用セルフ IP アドレスの作成 4-5
Web サーバのプールの作成 4-5
バーチャルサーバの作成 4-6

5
複数カスタマの Web ホスティング

複数カスタマのホスティングの概要 5-1
外部スイッチを使用した複数カスタマのホスティング 5-2
タグ付きインターフェイスを持つ VLAN の作成 5-2
ロードバランシングプールの作成 5-3
バーチャルサーバの作成 5-3
複数カスタマの直接ホスティング 5-5
タグなしインターフェイスを持つ VLAN の作成 5-6

6
単純なイントラネット設定

単純なイントラネット設定での作業 6-1
単純なイントラネット設定の作成 6-2

プールの作成 6-2
バーチャルサーバの作成 6-3

7
ISP のロードバランシング
ISP のロードバランシングの概要 7-1
ISP のロードバランシングの設定 7-2
追加インターネット接続用プールの作成 7-2
追加インターネット接続用バーチャルサーバの作成 7-3
発信トラフィックのアドレス変換の設定 7-5

8
送信元アドレスアフィニティパーシステンスを使用した HTTP トラフィックのロードバランシング
基本的な HTTP のロードバランシングの概要 8-1
送信元アドレスのアフィニティパーシステンスを使用した HTTP ロードバランシングの設定 8-2
プールの作成 8-2
バーチャルサーバの作成 8-3

9
Cookie パーシステンスを使用した HTTP トラフィックのロードバランシング
基本的な HTTP のロードバランシングの概要 9-1
Cookie パーシステンスを使用した HTTP ロードバランシングの設定 9-2
カスタム Cookie パーシステンスプロファイルの作成 9-2
プールの作成 9-3
バーチャルサーバの作成 9-4

10
HTTP 応答の圧縮
HTTP データ圧縮の概要 10-1
カスタム HTTP プロファイルの作成 10-2
バーチャルサーバの作成 10-3

11
HTTPS のロードバランシングの設定
HTTPS のロードバランシングの概要 11-1
SSL キーと証明書の作成 11-2
カスタム SSL プロファイルの作成 11-3
プールの作成 11-5
バーチャルサーバの作成 11-6

12
データ圧縮を使用した HTTPS のロードバランシングの設定
圧縮を使用した HTTPS のロードバランシングの概要 12-1
SSL キーと証明書の作成 12-2
カスタム Client SSL プロファイルの作成 12-3
圧縮用のカスタム HTTP プロファイルの作成 12-4
プールの作成 12-6
バーチャルサーバの作成 12-7

13
HTTP トラフィック用の RAM キャッシュの使用
HTTP RAM キャッシュの概要 13-1
カスタム HTTP プロファイルの作成 13-2

バーチャルサーバの作成 13-3

14
パッシブモードの FTP トラフィックのロードバランシング
FTP のロードバランシングの概要 14-1
カスタム FTP モニタの作成 14-2
プールの作成 14-3
バーチャルサーバの作成 14-4

15
レートシェイピングを使用したパッシブモードの FTP トラフィックのロードバランシング
レートシェイピングを使用した FTP のロードバランシングの概要 15-1
カスタム FTP モニタの作成 15-2
プールの作成 15-3
レートクラスの作成 15-4
バーチャルサーバの作成 15-5

16
単一 IP ネットワークトポロジのセットアップ
単一 IP ネットワークトポロジの概要 16-1
単一 IP ネットワークトポロジ用のプールの作成 16-2
バーチャルサーバの作成 16-3
デフォルトルートの定義 16-4
クライアント SNAT の設定 16-5

17
タグ付き VLAN でのリンクアグリゲーションの使用
タグ付き VLAN インターフェイスでのリンクアグリゲーションの概要 17-1
2 ネットワーク構成でアグリゲートしたタグ付きインターフェイストポロジの使用 17-2
リンクのアグリゲート 17-3
VLAN へのトランクの割り当て 17-3
ロードバランスする Web サーバのプールの作成 17-4
Web サーバをロードバランスするバーチャルサーバの作成 17-5
1 ネットワーク構成でのアグリゲートしたタグ付きインターフェイストポロジの使用 17-6
VLAN からのセルフ IP アドレスの削除 17-7
VLAN グループの作成 17-7
VLAN グループ用のセルフ IP アドレスの作成 17-8

18
パケットフィルタリングのセットアップ
パケットフィルタリングの概要 18-1
パケットフィルタリングの設定 18-2
SNAT の作成 18-2
ゲートウェイプールの作成 18-2
フォワーディングバーチャルサーバを作成する 18-3
パケットフィルタルールの作成 18-4

19
ヘルスモニタとパフォーマンスモニタの実装
ヘルスモニタとパフォーマンスモニタの概要 19-1
カスタムモニタの作成 19-3
プールの作成 19-4
プールへのモニタの割り当て 19-4

モニタからのプールメンバの除外 19-5
バーチャルサーバの作成 19-6

20
IPv6 ノードへのトラフィックのロードバランシング

radvd サービスの設定 20-1
IPv4 と IPv6 間のロードバランシングの設定 20-2
IPv6 ノードのプールの作成 20-2
バーチャルサーバの作成 20-3

21
重複した IP アドレスの実装

重複した IP アドレスの概要 21-1
ルートドメインとは 21-1
ルートドメイン ID の指定 21-1
ルートドメインの設定 21-3
ルートドメインに対する VLAN の作成 21-4
ルートドメインに対するセルフ IP アドレスの作成 21-6
ルートドメインオブジェクトの作成 21-7
ルートドメインに対するプールメンバの作成 21-8
スタティックルートの作成 21-9
ルートドメインに対するバーチャルサーバの作成 21-10

22
サービス拒否攻撃やその他の攻撃の緩和

基本的なサービス拒否攻撃に対するセキュリティの概要 22-1
アダプティブコネクションリーパの設定 22-2
アダプティブコネクションリーパの活動の記録 22-3
単純な DoS 攻撃の防御設定 22-4
TCP および UDP 接続タイマの設定 22-4
IP レートクラスの作成とバーチャルサーバへの適用 22-5
主要バーチャルサーバでの接続制限の設定 22-6
iRule を使用した攻撃のフィルタ除去 22-7
Code Red 攻撃のフィルタ除去 22-7
Nimda 攻撃のフィルタ除去 22-7
BIG-IP での、一般的なさまざまな攻撃への対処方法 22-8
SYN フラッド 22-8
ICMP フラッド（スマーフ） 22-9
UDP フラッド 22-9
UDP フラグメント 22-10
Ping of Death 22-10
Land 攻撃 22-10
Teardrop 22-11
データ攻撃 22-11
WinNuke 22-11
Sub 7 22-11
Back Orifice 22-12

23
管理ドメインの設定

管理ドメインの概要 23-1
パーティションの作成 23-2
パーティションに対するユーザアクセスの設定 23-3
パーティション内のオブジェクトの表示、管理、作成 23-4
システムオブジェクトの表示と管理 23-4
BIG-IP システムオブジェクトの作成 23-5

24
管理トラフィックのリモート認証および承認の設定

BIG-IP ユーザアカウントのリモート認証と承認の概要 24-1
BIG-IP でユーザアカウントのリモート認証を使用するための設定 24-2
BIG-IP ユーザのアクセス制御の設定 24-6
remoterole コマンドの概要 24-7
remoterole コマンドの使用 24-7
変数置換の使用 24-8
複数の BIG-IP へのリモート認証データとリモート承認データの伝播 24-11

25
アプリケーショントラフィックのリモート認証の設定

アプリケーショントラフィックのリモート認証の概要 25-1
リモート LDAP サーバまたは Active Directory サーバを使用する認証の設定 .. 25-2
LDAP 構成オブジェクトの作成 25-2
LDAP 認証プロファイルの作成 25-5
LDAP 認証用バーチャルサーバの変更 25-5
リモート RADIUS サーバを使用する認証の設定 25-7
RADIUS サーバオブジェクトの作成 25-7
RADIUS 構成オブジェクトの作成 25-8
RADIUS プロファイルの作成 25-9
RADIUS 認証用バーチャルサーバの変更 25-9
リモート TACACS+ サーバを使用する認証の設定 25-11
TACACS+ 構成オブジェクトの作成 25-11
TACACS+ プロファイルの作成 25-12
TACACS+ 認証用バーチャルサーバの変更 25-13
リモート LDAP サーバを使用した SSL ベースの承認の設定 25-14
SSL クライアント証明書 LDAP 構成オブジェクトの作成 25-14
SSL クライアント証明書 LDAP 認証プロファイルの作成 25-15
SSL クライアント証明書 LDAP 承認用バーチャルサーバの変更 25-16
OCSP レスポンダを使用した SSL 証明書失効の設定 25-17
SSL OCSP レスポンダオブジェクトの作成 25-17
SSL OCSP 構成オブジェクトの作成 25-18
SSL OCSP プロファイルの作成 25-18
SSL OCSP 認証用バーチャルサーバの変更 25-19
CRLDP 認証モジュールの設定 25-20
CRLDP サーバオブジェクトの作成 25-20
CRLDP 構成オブジェクトの作成 25-21
CRLDP プロファイルの作成 25-21
CRLDP 認証用バーチャルサーバの変更 25-22

26
Kerberos 委任の設定

Kerberos 委任インフラストラクチャの概要 26-1
BIG-IP での Kerberos 委任の設定 26-2
BIG-IP への DNS サーバの追加 26-2
信頼済みドメインへの BIG-IP の参加 26-3
Kerberos 委任設定の作成 26-4
設定ユーティリティを使用した Kerberos 委任の設定 26-4
コマンドラインからの Kerberos 委任の設定 26-7
クライアントトラフィックの認証 26-9

27
複数の認証サーバの設定

複数の認証サーバ設定の概要 27-1
前提条件 27-2
BIG-IP システムオブジェクトの設定 27-2

28
ペアトンネリングの実装

ペアトンネリングの実装 28-1
ペアトンネリングについて 28-1
データ圧縮について 28-2
準備 28-3
クライアント側 BIG-IP の設定 28-4
クライアント側エンドポイントプールの作成 28-4
クライアント側 iSession プロファイルの作成 28-5
クライアント側バーチャルサーバの作成 28-6
サーバ側 BIG-IP の設定 28-9
サーバ側バーチャルサーバの作成 28-10
サービスポートの指定 28-11
データ圧縮の統計情報の表示 28-12

29
ASM および WA による HTTP トラフィックのセキュリティ保護と高速化

設定タスクの概要 29-1
BIG-IP LTM での基本的な設定の完了 29-2
BIG-IP LTM での初期設定タスクの実行 29-3
HTTP クラスプロファイルの作成 29-3
BIG-IP LTM でのバーチャルサーバとプールの定義 29-4
NTP サーバの定義 29-6
WebAccelerator 用のアプリケーションプロファイルの作成 29-7
高速化ポリシーの選択 29-7
ホストマップの計画 29-8
Application Security Manager のセキュリティポリシーへの WebAccelerator アプリケーションプロファイルの割り当て 29-12
Application Security Manager の Deployment Wizard の実行 29-13

30
PSM および WA による HTTP トラフィックのセキュリティ保護と高速化

設定タスクの概要 30-1
BIG-IP LTM での基本的な設定の完了 30-2
BIG-IP LTM での初期設定タスクの実行 30-3
WebAccelerator HTTP クラスプロファイルの作成 30-3
HTTP サービスプロファイルの作成 30-4
BIG-IP LTM でのバーチャルサーバとプールの作成 30-5
WebAccelerator 用のアプリケーションプロファイルの作成 30-7
高速化ポリシーの選択 30-7
ホストマップの計画 30-8
Protocol Security Module 設定での HTTP セキュリティプロファイルの作成 30-12

用語集

索引

1

BIG-IP LTM の実装の概要

- BIG-IP 実装の概要
- 本ガイドについて
- ヘルプおよびテクニカルサポートリソースへのアクセス

BIG-IP 実装の概要

一般的な構成では、BIG-IP は、さまざまなタイプのプロトコルおよびアプリケーションのトラフィックを、適切な送信先サーバへダイレクトする、ネットワーク上のデバイスとして機能します。トラフィックをロードバランシングサーバプールへ直接転送する、トラフィックを特定サーバノードに直接送信する、ネクストホップルータまたはルータのプールへ送信することにより、この機能が実現しています。BIG-IP の最も基本的な構成では、2 つの仮想ローカルエリアネットワーク（VLAN）が設けられ、それぞれの VLAN に、BIG-IP インターフェイス（ポート）が割り当てられています。BIG-IP のブラウザベースの設定ユーティリティでは、デフォルトの VLAN 設定を使用して、カスタマイズされたバーチャルサーバ、トラフィックプロファイル、およびロードバランシングプールなどの BIG-IP システムオブジェクトを作成するだけで、多数の設定シナリオを実装できます。

◆注

*BIG-IP® LTM は、BIG-IP 製品ファミリを構成する一製品です。BIG-IP 製品ファミリのすべての製品は、TMOS™ とも呼ばれる、強力な Traffic Management Operating System で実行します。すべての BIG-IP 製品サービスの概要については、『**TMOS™ Management Guide for BIG-IP® Systems**』を参照してください。*

はじめに

本ガイドのソリューションの実装を開始する前に、他の BIG-IP ガイドやオンラインヘルプなど、その他のリソースを参照して、この章に記載されている表記規則を確認しておくことをお勧めします。詳細については、「*本ガイドについて*」（1-2 ページ）を参照してください。

また、BIG-IP 上でセットアップユーティリティを実行して、基本ネットワークと、静的およびフローティングセルフ IP アドレス、インターフェイス、VLAN などのネットワーク要素の設定を行っておくことをお勧めします。セットアップユーティリティを実行した後に、本ガイドを使用して特定の設定シナリオを実装します。設定ユーティリティの実行については、『***BIG-IP® Systems: Getting Started Guide***』を参照してください。

設定ユーティリティの使用

セットアップユーティリティを実行したら、設定ユーティリティで各自の設定に必要な追加作業を行います。設定ユーティリティの使用については、『***BIG-IP® Systems: Getting Started Guide***』を参照してください。

設定ユーティリティでサポートされるブラウザのバージョンについては、F5 Prime Members Web サイト（**https://www.f5networks.co.jp/primemembers/**）に掲載されている本製品のリリースノートをご覧ください。

本ガイドについて

本ガイドでは、それぞれの章で、設定ユーティリティを使用して完全なトラフィック管理ソリューションを実装するための段階的な手順について説明しています。たとえば、第 3 章「*Web サイトおよび電子商取引の基本設定*」」では、電子商取引のトラフィックを処理する一連の Web サーバのセットアップに必要な BIG-IP システムオブジェクトの設定方法について説明しています。

補足情報

本ガイド以外にも、BIG-IP の操作に関する資料が用意されています。次のガイドは、F5 Prime Members Web サイト（**https://www.f5networks.co.jp/primemembers/**）で提供されています（PDF 版）。

- 『***BIG-IP® Systems: Getting Started Guide***』
  このガイドには BIG-IP のライセンスとプロビジョニング、およびアップグレードのインストールに関する詳細情報が記載されています。また、BIG-IP の機能およびシステム設定ツールについて簡単に説明しています。
- 『***TMOS™ Management Guide for BIG-IP® Systems***』
  このガイドには、ルータ、VLAN、ユーザアカウントなど、BIG-IP のネットワークおよびシステム関連コンポーネントを設定するために必要な情報が記載されています。
- 『***Configuration Guide for BIG-IP® Local Traffic Management***』
  このガイドには、ローカルネットワークトラフィックを管理できるように BIG-IP の特定の機能を設定する場合に必要なすべての情報が記載されています。
- 『***BIG-IP® Application Security Manager: Getting Started Guide***』
  このガイドには、BIG-IP Application Security Manager をセットアップしてセキュリティポリシーを設定する方法について記載されています。
- 『***Configuration Guide for BIG-IP® Protocol Security Module***』
  このガイドには、BIG-IP Protocol Security Module の設定手順について記載されています。
- 『***Configuration Guide for the BIG-IP® WebAccelerator™ System***』
  このガイドには、BIG-IP WebAccelerator の基本概念、および WebAccelerator の設定や監視手順について記載されています。
- 『***Bigpipe Utility Reference Guide***』
  このガイドには、**bigpipe** ユーティリティコマンドを使用した BIG-IP の管理について記載されています。
- 『***Traffic Management Shell (tmsh) Reference Guide***』
  このガイドには、Traffic Management Shell（**tmsh**）コマンドを使用した BIG-IP の管理について記載されています。

表記規則

重要な情報を簡単に特定したり理解できるように、すべてのドキュメントはこの表記規則に従って記されています。

例の使用

本ドキュメントでは、すべての例にプライベートクラスの IP アドレスのみを使用しています。記載された実装を設定するときには、サンプルのアドレスの代わりに、ユーザ自身のネットワークに適した有効な IP アドレスを使用する必要があります。

新規用語の識別

定義されている用語を識別しやすいように、該当用語を太字の斜体で表記しています。例：***フローティング IP アドレス***は、VLAN に割り当てられ、2 台のコンピュータシステム間で共有されている IP アドレスを表します。

製品への参照の識別

BIG-IP 製品ファミリのすべての製品を BIG-IP と呼びます。ソフトウェアモジュールはその名前で呼びます。たとえば、BIG-IP Local Traffic Manager は BIG-IP LTM と呼びます。設定情報が特定のハードウェアプラットフォームに関連している場合は、そのプラットフォームを記しています。

オブジェクト、名前、コマンドへの参照の識別

文中で識別しやすいように、さまざまな項目を太字で表記しています。Web アドレス、IP アドレス、ユーティリティ名、変数やキーワードといったコマンドの一部などが太字になっていることがあります。例：**bigpipe self <ip_address> show** コマンドでは、**<ip_address>** 変数に IP アドレスを指定することにより、表示する特定のセルフ IP アドレスを指定できます。

他のドキュメントへの参照の識別

別のドキュメントまたは特定の項への参照は、斜体で表記しています。書籍タイトルへの参照は、太字の斜体で表記しています。
例：インストールについては、『***BIG-IP® Systems: Gettng Started Guide***』*を参照してください。*

コマンド構文の識別

完全なコマンドは、太字の Courier 文字で表示しています。コマンド行画面全体を表示するコマンドでない場合は、該当する画面プロンプトにこの表記規則は当てはまらないので注意してください。

たとえば次のコマンドは、指定されたプール名の設定を示します。

```
bigpipe self <ip_address> show
```

もしくは

```
b self <ip_Address> show
```

表 1.1 では、コマンド行構文で使用されるその他の特別な表記規則について説明しています。

テキスト内の項目	説明
\	コマンドが次の行に続き、改行を入れずにコマンド全体を入力することを示します。
< >	ユーザ定義のパラメータを示します。たとえば、コマンドに **<your name>** とある場合、ユーザの名前を入力します。括弧は取ります。
|	コマンドを分割します。
[]	括弧内の構文がオプションであることを示します。
...	一連の項目を入力できることを示します。

表 1.1 *コマンド行構文の表記規則*

ヘルプおよびテクニカルサポートリソースへのアクセス

追加のテクニカルドキュメントおよび製品情報は、次の場所で入手できます。

- **ローカルトラフィック管理のオンラインヘルプ**
  設定ユーティリティには、画面ごとにオンラインヘルプがあります。オンラインヘルプから、画面上の各コントロールおよび設定の説明を表示できます。左側のナビゲーションペインの [Help] タブをクリックすると、オンラインヘルプが表示されます。
- **設定ユーティリティの [Welcome] 画面**
  設定ユーティリティの [Welcome] 画面には、次のような便利な Web サイトおよびリソースへのリンクが数多く含まれています。
  - F5 Networks Technical Support Web サイト（英語のみ）
  - F5 Solution Center（英語のみ）
  - F5 DevCentral Web サイト
  - プラグイン、SNMP MIB、および SSH クライアント
- **F5 Prime Members Web サイト**
  日本のお客様には、F5 Prime Members Web サイト（**https://www.f5networks.co.jp/primemembers/**）より、以下の最新製品ドキュメントを提供しています。
  - 各製品の新旧リリースノート
  - 各製品ガイド
  - 【削除】テクニカルノート
  - 【削除】FAQ（よくある質問）への回答
  - The Ask F5[SM] Knowledge Base

  このサイトにアクセスするには、**http://www.f5networks.co.jp/f5pm** での登録が必要です。

2

nPath ルーティングの設定

- nPath ルーティングの概要
- nPath ルーティングの設定
- nPath 設定用のタイマの設定

nPath ルーティングの概要

nPath ルーティング設定を使用すると、発信するサーバトラフィックを、BIG-IP を回避して発信ルータへ直接転送できます。このトラフィック管理方式の場合、変換とネクストホップへの転送のためにパケットを BIG-IP へ送信する必要がないので、送信スループットが増加します。図 2.1 は、nPath 構成を示しています。

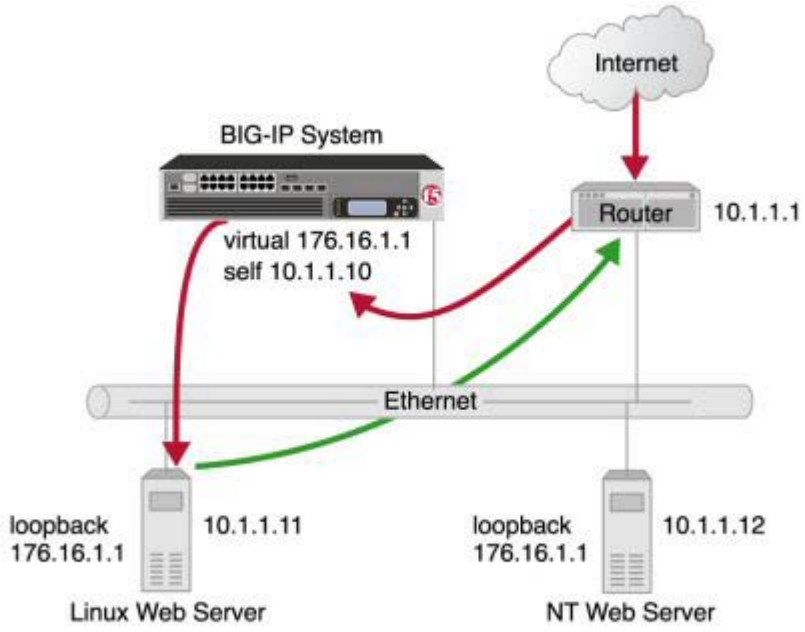

***図 2.1** nPath 実装の例*

◆注

着信トラフィックを処理するバーチャルサーバは、透過的で変換を行わないタイプのバーチャルサーバであることが必要です。

戻り パス上で BIG-IP を迂回する場合、nPath ルーティングは、通常のロード バランシング設定とは著しく異なります。一般的なロード バランシング設定では、着信パケットの宛先アドレスは、バーチャルサーバのアドレスからロード バランス先のサーバのアドレスへ変換され、続いてこのアドレスが戻りパケットの送信元アドレスになります。BIG-IP に設定されたデフォルトのルートでは、発信元クライアントへ戻るパケットが、BIG-IP を中継して戻るように設定されており、BIG-IP で送信元アドレスがバーチャルサーバのアドレスに再変換されます。nPath 設定は、次の項で説明するように、一般的なロード バランシング設定とは異なります。

◆注

nPath ルーティングは、レイヤ 7 トラフィックには使用しないでください。レイヤ 7 トラフックが戻りパス上で BIG-IP を迂回すると、特定のトラフィック機能が正しく動作しません。たとえば、HTTP 応答圧縮などの機能が正しく動作しません。

nPath ルーティングの設定

nPath ルーティングの設定は、次の点で一般的な BIG-IP ロードバランシング設定と異なります。

- コンテンツサーバでのデフォルト ルート は、BIG-IP のフローティングセルフ IP アドレス（図 2.1（2-1 ページ）の **10.1.1.10**）ではなく、ルータの内部アドレス（**10.1.1.1**）に設定する必要があります。これで、戻りパケットは BIG-IP を迂回します。
- TCP トラフィックに nPath 構成を使用する場合は、次のカスタム設定で Fast L4 プロファイルを作成します。
  - **Loose Close** 設定を有効にします。**Loose Close** 設定を有効にすると、TCP プロトコルフローは、TCP FIN パケットが見つかるとすぐに失効します（***FIN パケット***は、これまでの接続の切断を指示します）。
  - ハーフクローズが必要な場合は、**[TCP Close Timeout]** 設定をプロファイルのアイドルタイムアウトと同じ値に設定しますが、そうでない場合は、この値を 5 秒に設定します。
- アドレス変換とポート変換は無効になっているので、着信パケットは、サーバのアドレスではなくバーチャルサーバのアドレス（図 2.1（2-1 ページ）の **176.16.1.1**）を使用して、着信パケットのロードバランシング先のプールメンバに到達します。サーバがそのアドレスに応答するには、このアドレスが、サーバのループバックインターフェイスで設定され、サーバソフトウェアで使用できるように設定されている必要があります。

BIG-IP で nPath ルーティングを使用するように設定するには、次の作業を完了する必要があります。

- カスタムの Fast L4 プロファイルを作成する
- コンテンツサーバを含んだプールを作成する
- ポートおよびアドレス変換を無効にしてバーチャルサーバを定義し、カスタムの Fast L4 プロファイルをそのサーバに割り当てる
- それぞれのサーバのループバックインターフェイスで、バーチャルサーバアドレスを設定する
- ルータの内部 IP アドレスまでのデフォルトルートをサーバ上で設定する
- bigdb 設定キー **connection.autolasthop** が有効になっていることを確認します。また、各コンテンツサーバで、クライアントへの戻りルートを追加できます。

これらの作業の詳細については、設定ユーティリティの [Help] タブまたは『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

◆注

このガイドに記載されている作業を、設定ユーティリティを使用して実行します。ただし、この手順には、設定ユーティリティのログイン手順は含まれていません。これらの作業を開始する前に、設定ユーティリティにログオンしてください。

カスタムの Fast L4 プロファイルの作成

nPath ルーティング設定の作成では、最初に、カスタムの Fast L4 プロファイルを作成します。

カスタムの Fast L4 プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. Protocol メニューから、Fast L4 を選択します。
   [Fast L4 Profiles] 画面が開きます。
3. カスタムプロファイルを作成するには、[**Create**] をクリックします。
   [New Fast L4 Profile] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではFast L4 プロファイルを作成する権限が与えられていないことを示します。*
4. [New Fast L4 Profile] 画面で、次の属性を設定します。
   a) [**Name**] ボックスに、プロファイルの名前を入力します。
   b) [**Loose Close**] ボックスをオンにします。
   c) バーチャルサーバが処理するトラフィックのタイプに従って、[**TCP Idle Timeout**] 設定を定めます。このタイムアウトの設定の詳細については、「*nPath 設定用のタイマの設定*」（2-6 ページ）を参照してください。
5. [**Finished**] をクリックします。

nPath ルーティング用のサーバプールの作成

カスタムの Fast L4 プロファイルを作成した後、サーバプールを作成する必要があります。

プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 新しいプールを作成するには、[**Create**] をクリックします。
   [New Pool] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. プール名を入力して、サーバごとにメンバアドレスを追加します
4. [**Finished**] をクリックします。

バーチャルサーバの作成

サーバプールを作成した後、前の 2 つの作業で作成したカスタム Fast L4 プロファイルとプールを参照するバーチャルサーバを作成する必要があります。

標準バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 新しいバーチャルサーバを作成するには、[**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. バーチャルサーバ名を入力し、宛先タイプを選択して、IP アドレスを入力します。
4. [**Type**] 設定から [**Performance (Layer 4)**] を選択します。
5. 次の属性を設定します。
   a) [**Protocol**] のリストから **[UDP]、[TCP]、または [*All Protocols**] のいずれかを選択します。
   b) [**Protocol Profile (Client)**] では、作成したカスタム Fast L4 プロファイルを選択します。
   c) [**Address Translation**] チェックボックスをオフにして、アドレス変換を無効にします。

d) [**Port Translation**] チェックボックスをオフにして、ポート変換を無効にします。

e) Resources のセクションから、コンテンツサーバを含む作成済みプールを選択します。

6. [**Finished**] をクリックします。

コンテンツサーバのループバックインターフェイスでのバーチャルサーバアドレスの設定

バーチャルサーバの IP アドレス（2-1 ページの図 2.1 の **176.16.1.1**）を、各サーバのループバックインターフェイスで設定する必要があります。ほとんどの UNIX 系システムには、**lo0** という名前のループバックインターフェイスが用意されています。Microsoft® Windows® では、ネットワークアダプタのリスト内に、MS Loopback インターフェイスが用意されています。Windows のバージョンによっては、インストール CD を使用してループバックインターフェイスをインストールする必要があります。ループバックインターフェイスでの IP アドレスの設定については、サーバのオペレーティングシステムのドキュメントを参照してください。ループバックインターフェイスは、ARP プロトコルに関与しないので、nPath 設定には理想的です。

着信トラフィック用ルートの設定

着信トラフィックに対して、BIG-IP のセルフ IP アドレスを使用してバーチャルサーバへ到達するルートを定義する必要があります。例では、このルートは **176.16.1.1** であり、ゲートウェイとして外部セルフ IP アドレス **10.1.1.10** を使用します。

◆注

このルートは、バーチャルサーバがルータ以外のサブネットにある場合にのみ設定する必要があります。

このルートの定義方法の詳細については、ルータに付属のドキュメントを参照してください。

connection.autolasthop bigdb キーの有効化

npath ルーティングが正しく機能するためには、bigdb 設定キー **connection.autolasthop** が **enable** に設定されていなければなりません。これは、IPv4 および IPv6 の両方のアドレスフォーマットに関連します。

この bigdb キーを有効にするには、次のコマンドを入力します。

```
bigpipe db connection.autolasthop enable
```

nPath 設定用のタイマの設定

nPath 設定を作成すると、BIG-IP はクライアントの要求しか認識しません。したがって、接続タイムアウトのタイマは、クライアントが送信してきたときにのみリセットされます。一般に、BIG-IP がクライアントの要求とノードの応答の両方を認識する場合の同様の接続であれば、nPath 接続のタイムアウトの時間が少なくとも 2 倍になることになります。以下に、UDP トラフィックと TCP トラフィックでの、タイマ設定のシナリオを説明します。

UDP トラフィックでのタイムアウトの設定ガイドライン

UDP トラフィック用に nPath を設定すると、BIG-IP は、同じ送信元および宛先アドレス間で送信されたパケットを、接続と同じ宛先ポートまで追跡します。これは、セッションの一部であるクライアント要求が常に同じサーバに到達するために必要です。したがって、UDP はコネクションレス型のプロトコルであるため、UDP 接続は実際にパーシステンスの形式になります。UDP のタイムアウトを計算するために、クライアントがパケットを送信するまでに、サーバが UDP パケットを送信する最大時間を見積もります。サーバは、セッションが終わるまでの間、またはクライアントの応答を待つ間に数分間にわたって数百のパケットを送信する場合があります。

TCP トラフィックでのタイムアウトの設定ガイドライン

TCP トラフィックの nPath を設定するときに、BIG-IP は接続のクライアント側しか認識しません。たとえば、TCP 3 ウェイハンドシェイクでは、BIG-IP は、クライアントからサーバへの SYN を認識し、サーバからクライアントへの SYN 確認応答は認識せず、クライアントからサーバへの確認応答に対する確認応答を認識します。接続のタイムアウトは、すべての接続が正常に行われるように、クライアントとノードの TCP 再送信タイムアウト（RTO）の組み合わせにできるだけ近似する必要があります。多くの UNIX および Windows システムで見られる最大初期 RTO は、約 25 秒です。したがって、51 秒のタイムアウトは、最悪の場合にも十分対応できます。TCP セッションが確立されると、適応可能なタイムアウトが使用されます。ほとんどの場合、このタイムアウトがクライアントおよびノードで最速になります。クライアントが低速で損失の多いネットワーク上に存在する場合にのみ、より高い TCP タイムアウトを設定する必要があります。

3

Web サイト および電子商取引の基本設定

- Web サイトおよび電子商取引の基本設定での作業
- 基本的な電子商取引サイトの設定

Web サイト および電子商取引の基本設定での作業

BIG-IP システムは、通常、電子商取引トラフィックなどの標準的な Web トラフィックをホストする一連の Web サーバにトラフィックを分散させるのに使用します。図 3.1 は、BIG-IP が **www.siterequest.com** および **store.siterequest.com** の 2 つのサイトをロードバランスしている構成を示しています。**www.siterequest.com** サイトは、標準的な Web コンテンツを提供しており、**store.siterequest.com** サイトは、**www.siterequest.com** の顧客に商品を販売している電子商取引サイトです。

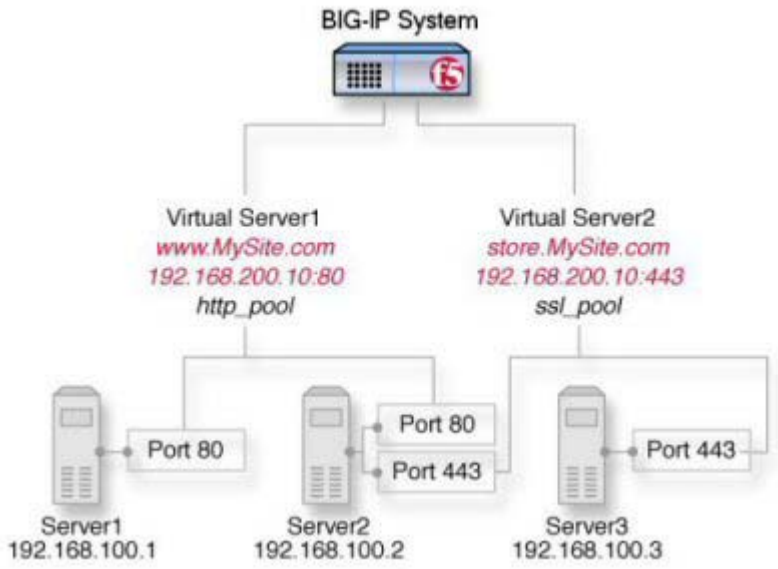

図 3.1 *基本的なロードバランシング設定*

これらのサイトに対してロードバランシングを設定するには、各サイトに 1 つずつ、バーチャルサーバが参照するプールを作成する必要があります。**www.siterequest.com** へ送信される HTTP トラフィックにはポート **80**、**store.siterequest.com** へ送信される SSL トラフィックにはポート **443** というように、それぞれのサイトで異なるポートを使用して特定のプロトコルをサポートするため、両方のサイト間に関連性があり、同じ IP アドレスを共有している場合でも、それぞれのサイトに固有のバーチャルサーバが必要です。これは **Server2** の場合のように、ポート **80** とポート **443** が同じ物理サーバ上にある場合にも該当することに注意してください。

◆注

本ドキュメントでは、すべての例にプライベートクラスの IP アドレスのみを使用しています。記載されている設定をセットアップする場合は、サンプルアドレスの代わりに、ユーザ自身のネットワークに適した有効な IP アドレスを使用してください。

基本的な電子商取引サイトの設定

電子商取引サイトを設定するには、次の作業を順番に完了する必要があります。

- **ロードバランシングプールを作成する**
  HTTP 接続をロードバランスするためのプール、および SSL 接続をロードバランスするためのプールを作成します。
- **着信トラフィック用のバーチャルサーバを作成する**
  HTTPおよびSSLプールを参照するバーチャルサーバを作成します。

ロードバランシングプールの作成

基本設定では、まず、HTTP 接続をロードバランスするプールと、SSL 接続をロードバランスするプールの 2 つのプールを定義します。図 3.1（3-1 ページ）に示すように、HTTP プール用の 2 台のサーバは、**192.168.100.1:80** と **192.168.100.2:80** です（**Server1** と **Server2**）。SSL プール用の 2 台のサーバは、**192.168.100.2:443** と **192.168.100.3:443** です（**Server2** と **Server3**）。

設定ユーティリティを使用して、これらの 2 つのプールを作成します。プールの設定の詳細については、オンラインヘルプを参照してください。

HTTPトラフィックのロード バランシング用プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   ***注**: [Create] ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、プールの名前を入力します。
   図 3.1（3-1 ページ）の例では、このプール名は **http_pool** です。
4. 画面の [Resources] 領域で、[**New Members**] 設定を使用してプールメンバを追加します。
   図 3.1（3-1 ページ）の例では、このプールメンバは **192.168.100.1:80** と **192.168.100.2:80** です。
5. [**Finished**] をクリックします。

SSL トラフィックのロードバランシング用プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。

3. [**Name**] ボックスに、プールの名前を入力します。
図 3.1（3-1 ページ）の例では、このプール名は **ssl_pool** です。
4. 画面の [Resources] 領域で、[**New Members**] 設定を使用してプールメンバを追加します。
図 3.1（3-1 ページ）の例では、このプールメンバは **192.168.100.2:443** と **192.168.100.3:443** です。
5. [**Finished**] をクリックします。

バーチャルサーバの作成

基本設定の次の作業では、HTTP および SSL プールをそれぞれ参照するバーチャルサーバを定義します。設定ユーティリティを使用して、これらのバーチャルサーバを作成します。バーチャルサーバの設定の詳細については、[**Help**] ボタンをクリックしてください。

HTTP トラフィック用バーチャルサーバの定義方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
[Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
[New Virtual Server] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_http** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスにバーチャルサーバの IP アドレス（**192.168.200.10:80** など）を入力します。
5. [**Service Port**] ボックスに **80** と入力するか、リストから [**HTTP**] を選択します。
6. 画面の [Configuration] 領域で、[**HTTP Profile**] 設定を探して [**http**] を選択します。
7. 画面の [Resources] 領域で、[**Default Pool**] 設定を探して [**http_pool**] を選択します。
8. [**Finished**] をクリックします。

SSL トラフィック用バーチャルサーバの定義方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
[Virtual Servers] 画面が開きます。

2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*

3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_ssl** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスにバーチャルサーバの IP アドレス（**192.168.200.10:443** など）を入力します。
5. [**Service Port**] ボックスに **443** と入力するか、リストから [**HTTPS**] を選択します。
6. 画面の [Configuration] 領域で、[**SSL Profile (Client)**] 設定を探して [**clientssl**] を選択します。
7. 画面の[Resources]領域で、[**Default Pool**]設定を探して[**ssl_pool**] を選択します。
8. [**Finished**] をクリックします。

4

IP ネットワークを変更しない BIG-IP のインストール

- IP ネットワークを変更しない BIG-IP のインストール
- 同じ IP ネットワークの BIG-IP の設定

IP ネットワークを変更しない BIG-IP のインストール

BIG-IPの複数の機能を組み合わせることにより、既存のIPネットワークを変更せずに、BIG-IP をネットワーク内に配置できます。

図 4.1 は、BIG-IP を追加する前の、データセンターのトポロジを示しています。データセンターには、1 つの IP ネットワーク **10.0.0.0** を使用した LAN が 1 つあります。データセンターには、インターネットに接続した 1 台のルータ、2 台の Web サーバ、およびバックエンドのメールサーバが備えられています。

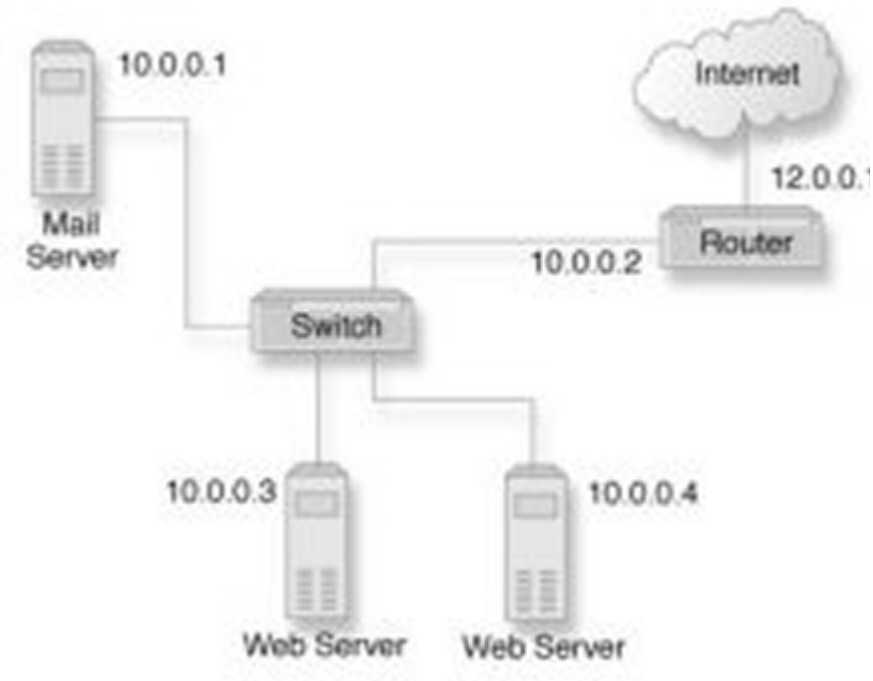

図 4.1 *既存のデータセンターのネットワーク構造*

既存のデータセンター構造では、ロードバランシングやハイアベイラビリティはサポートされていません。図 4.2（4-2 ページ）は、BIG-IP を追加した後の、データセンターのトポロジの例です。

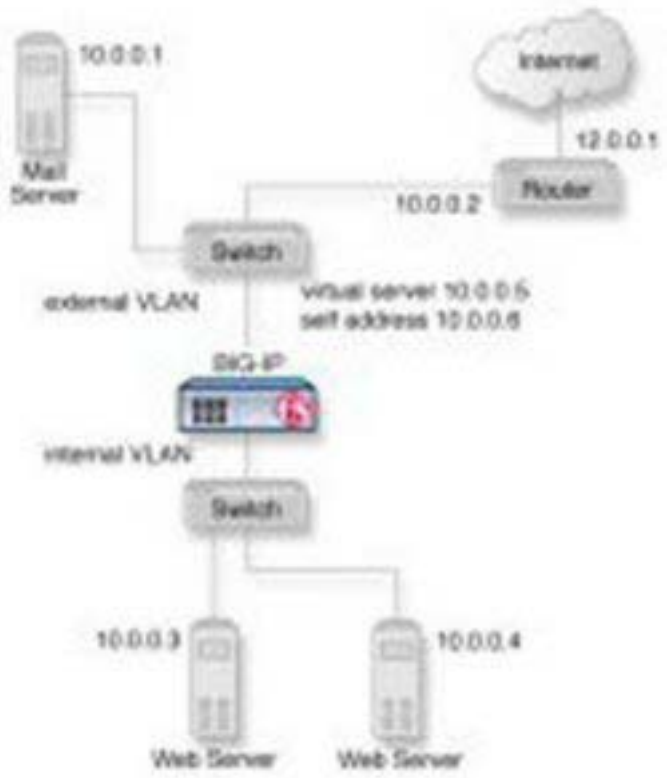

図 4.2 BIG-IP を追加した新しい構造

BIG-IP の内部および外部の両方のインターフェイスは、同じ IP ネットワーク **10.0.0.0** にありますが、実際は異なる LAN 上に置かれています。

図 4.2 では、第 2 のスイッチが導入されています。このスイッチは、BIG-IP を使用した構成では排除されます。

同じ IP ネットワークの BIG-IP の設定

この実装に BIG-IP を設定するには、VLAN グループ、Web サーバのプール、およびバーチャルサーバを作成する必要があります。具体的に、次の作業を行います。

- **個々の VLAN からセルフ IP アドレスを削除する**
  ルーティングは、VLAN グループ用に作成したセルフ IP アドレスによって処理されます。
- **VLAN グループを作成する**
  内部 VLAN と外部 VLAN を含む VLAN グループを作成します。これで、レイヤ 2 フォワーディングが有効になります（レイヤ 2 フォワーディングにより、2 つの VLAN は単一のネットワークのように動作します）。
- **VLAN グループ用のセルフ IP を作成する**
  VLAN グループ用のセルフ IP は、ネットワークに宛てられたパケットにルートを与えます。
- **Web サーバのプールを作成する**
  ロードバランスする Web サーバを含めたプールを作成します。
- **バーチャルサーバを作成する**
  Web サーバをロード バランスするバーチャルサーバを作成します。

◆注

*この例では、BIG-IP をインストールする同じ IP ネットワーク上にあるそれぞれの VLAN で、セルフ IP アドレスを持つデフォルトの **内部**および**外部** VLAN 設定を使用していることを前提としています。*

◆重要

*各コンテンツサーバでのデフォルトルートは、ルータの IP アドレスに設定します。この例では、デフォルトルートを **10.0.0.2** に設定しています。*

個々の VLAN からのセルフ IP アドレスの削除

個々の VLAN からセルフ IP アドレスを削除します。VLAN グループを作成し、ルーティング用に VLAN グループ用の別のセルフ IP アドレスを作成します。作成後は、VLAN ごとのセルフ IP アドレスは不要になります。

◆警告

この作業は、コンソールから、または削除しないセルフ IP アドレスから実行してください。削除するセルフ IP アドレスを通じてリモートのワークステーションから接続されている場合は、そのセルフ IP アドレスを削除すると接続が切断されます。

デフォルト VLAN からのセルフ IP アドレスの削除方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Self IPs**] をクリックします。
   [Self IPs] 画面が開きます。
2. IP Address カラムと VLAN カラムから、**内部** VLAN と**外部** VLAN のセルフ IP アドレスを探します。
3. 削除するセルフ IP アドレスの左側の [Select] ボックスをオンにします。

   ***注 : [Delete]** ボタンをクリックできない場合は、現在のユーザロールではセルフ IP アドレスを削除する権限が与えられていないことを示します。*
4. [**Delete**] をクリックします。
   確認画面が表示されます。
5. もう一度、[**Delete**] をクリックします。

VLAN グループの作成

内部 VLAN と外部 VLAN を含む VLAN グループを作成します。VLAN グループ内の VLAN が受信したパケットは、グループ内の他の VLAN にコピーされます。これでトラフィックは、同じ IP ネットワーク上の BIG-IP を通過できるようになります。

VLAN グループを作成するには

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**VLANs**] をクリックします。
   [VLANs] 画面が開きます。
2. [VLAN Groups] メニューから、[List] を選択します。
   [VLAN Groups] 画面が開きます。
3. 画面右上の [**Create**] をクリックします。
   [New VLAN Group] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールでは VLAN グループを作成する権限が与えられていないことを示します。*
4. [**Name**] ボックスに、グループ名 **myvlangroup** を入力します。
5. [**VLANs**] 設定では、[**Available**] ボックスから、**内部** VLAN および**外部** VLAN の名前を選択し、Move ボタン（<<）をクリックして、これらの VLAN 名を [**Selected**] ボックスに移動します。
6. [**Finished**] をクリックします。

VLAN グループ用セルフ IP アドレスの作成

VLAN グループ用のセルフ IP アドレスは、ネットワークに宛てられたパケットにルートを与えます。BIG-IP を使用した場合、IP ネットワークへのパスは VLAN です。ただし、この例で使用した VLAN グループ機能では、IP ネットワーク **10.0.0.0** へのパスは、実際には複数の VLAN を経由します。IP ルータは、ネットワークへの物理ルートを1つしか指定できないので、ルーティング衝突が発生します。BIG-IP でのセルフ IP アドレス機能は、セルフ IP アドレスを VLAN グループ上に設定することにより、ルーティング衝突を解消できます。

VLAN グループ用セルフ IP の作成方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Self IPs**] をクリックします。
   [Self IPs] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではセルフ IP アドレスを作成する権限が与えられていないことを示します。*
3. [**IP Address**] ボックスに、VLAN グループ用のセルフ IP を入力します。
   図 4.2（4-2 ページ）で示されている例では、この IP アドレスは **10.0.0.6** です。
4. [**Netmask**] ボックスに、セルフ IP アドレスのネットマスクを入力します。
5. [**VLAN**] 設定で、リストから名前の [**myvlangroup**] を選択します。
6. [**Finished**] をクリックします。

Web サーバのプールの作成

BIG-IP 用のネットワーク環境を作成してから、ロードバランスする Web サーバのプールを作成します。

プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、プールの名前（**myweb_pool** など）を入力します。

4. 画面の [Resources] 領域で、[**New Members**] 設定を使用してプールメンバを追加します。
   ここでの例では、プールメンバは**10.0.0.3:80**と**10.0.0.4:80**です。
5. [**Finished**] をクリックします。

バーチャルサーバの作成

ロードバランスする Web サーバのプールを作成してから、バーチャルサーバを作成します。

バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_myweb** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、IP アドレスを入力します。
   ここでの例を続けていくと、このアドレスは **10.0.0.5** になります。
5. [**Service Port**] リストから、[***All Ports**] を選択します。
6. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、前の手順を使用して作成したプールの名前を選択します。
   ここでの例では、プール名は **myweb_pool** です。
7. [**Finished**] をクリックします。

5

複数カスタマの Web ホスティング

- 複数カスタマのホスティングの概要
- 外部スイッチを使用した複数カスタマのホスティング
- 複数カスタマの直接ホスティング

複数カスタマのホスティングの概要

BIG-IP を使用して、ホスティングサービスを複数カスタマに提供し、ロードバランスができます。

図 5.1 の例では、BIG-IP は、ネットワーク上の 3 つの VLAN に割り当てられたインターフェイス（5.1）を備えています。VLAN は、**vlanA**、**vlanB**、および **vlanC** の 3 つです。インターフェイス 5.1 は 3 つの VLAN すべてのトラフィックを処理します。各 VLAN には 2 台のサーバがあり、特定のカスタマにサービスを提供しています。

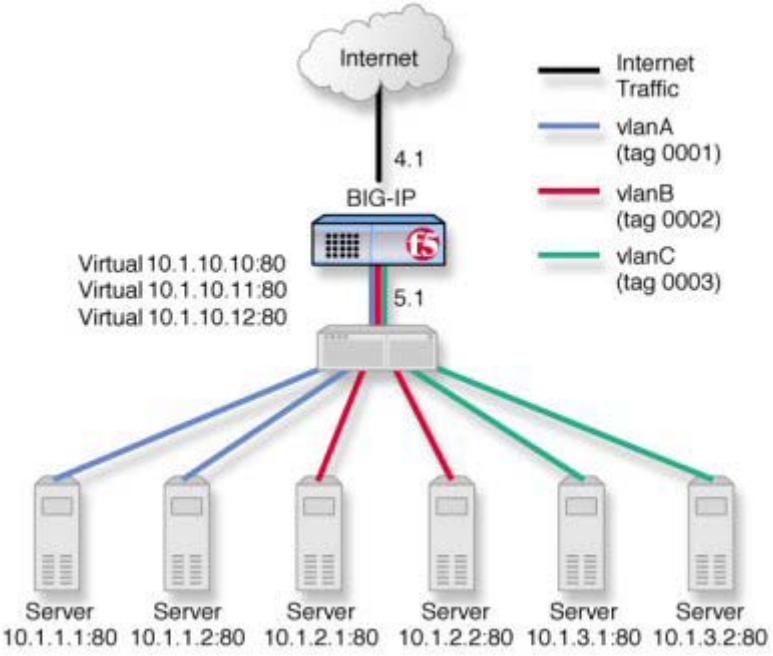

***図 5.1** 複数サイトのホスティングの例*

外部スイッチを使用した複数カスタマのホスティング

この実装に BIG-IP を設定するには、次の作業を完了する必要があります。

- タグ付きインターフェイスを持つ VLAN を作成する
  タグ付きインターフェイスの詳細については、『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください。
- ロードバランシングプールを作成します。
  トラフィックをロードバランスする対象の Web サーバのプールを、各 VLAN に 1 つずつ、合計 3 つ作成します。
- バーチャルサーバを作成します。
  Web サーバのプールへのトラフィックをロードバランスするバーチャルサーバを 3 つ作成します。

タグ付きインターフェイスを持つ VLAN の作成

BIG-IP で複数カスタマのホスティングを設定する場合、まず、タグ付きインターフェイスを持つ VLAN を作成します。この手順では、同一のインターフェイスを、作成するそれぞれの VLAN に割り当て、そのインターフェイスをタグ付きインターフェイスとして割り当てます （タグ付きインターフェイスの詳細については、『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください）。

たとえば、図 5.1（5-1 ページ）では、3 つの VLAN があり、各 VLAN が異なるサブネットのトラフィックを処理しています。つまり、**vlanA** は **10.1.1** サブネットのトラフィック、**vlanB** は **10.1.2** サブネットのトラフィック、**vlanC** は **10.1.3** サブネットのトラフィックを処理します。3 つの VLAN のすべてにインターフェイス 5.1 が割り当てられています。

タグ付きインターフェイスを持つ VLAN の作成方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**VLANs**] をクリックします。
   [VLAN] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   VLAN の設定が表示されます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールでは VLAN を作成する権限が与えられていないことを示します。
3. VLAN の名前とタグ番号を入力します。
   タグ番号を入力しないと、BIG-IP によって自動的に番号が生成されます。図 5.1（5-1 ページ）では、VLAN の名前を **vlanA**、タグ番号を **0001** として一例をあげています。

4. [**Interfaces**]設定では、[**Available**]ボックスから内部ネットワーク上のインターフェイスの名前を選択し、Move ボタン（<<）をクリックして、インターフェイスの名前を [**Tagged**] ボックスに移動します。
[Tagged] ボックスへの移動が完了すると、選択したインターフェイスがタグ付きインターフェイスとして VLAN に割り当てられます。この例では、インターフェイスは 5.1 です。
5. [**Finished**] をクリックします。

ロードバランシングプールの作成

BIG-IP 用の VLAN を作成したら、各 VLAN に 1 つずつ、合計 3 つのロードバランシングプールを作成します。図 5.1（5-1 ページ）では、各プールに 2 つのプールメンバが割り当てられています。

プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
[Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
[New Pool] 画面が開きます。
注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、プールの名前（**customerA_pool** など）を入力します。
4. 画面の [Resources] 領域で、[**New Members**] 設定を使用してプールメンバを追加します。
たとえば、図 5.1（5-1 ページ）では、**vlanA** のプールメンバは **10.1.1.1:80** と **10.1.1.2:80** です。**vlanB** のプールメンバは、**10.1.2.1:80** と **10.1.2.2:80** であり、**vlanC** のプールメンバは、**10.1.3.1:80** と **10.1.3.2:80** です。
5. [**Finished**] をクリックします。

バーチャルサーバの作成

ロードバランスする対象の Web サーバプールを作成したら、プールごとにバーチャルサーバを作成します。

バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
[Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
[New Virtual Server] 画面が開きます。

注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。

3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_customerA** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスにバーチャルサーバの IP アドレス（**10.1.10.10:80** など）を入力します。
5. [**Service Port**] ボックスに **80** と入力するか、リストから [**HTTP**] を選択します。
6. 画面の [Configuration] 領域で、[**HTTP Profile**] 設定を探して [**http**] を選択します。
7. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、作成しているバーチャルサーバに対応するプールを選択します。たとえば、**vs_customerA** に対しては、プール **customerA_pool** を選択します。**vs_customerB** に対しては、プール **customerB_pool** を選択します。
8. [**Finished**] をクリックします。

複数カスタマの直接ホスティング

図 5.1（5-1 ページ）の構成では、BIG-IP とサーバノード間で外部スイッチを使用しています。ただし、このソリューションの実装には、外部スイッチを取り除き、その代わりに BIG-IP 上で複数のインターフェイスを使用して、複数のカスタマに対してトラフィックを直接ホストする別の方法があります。このシナリオを使用する場合、VLAN の設定は必要ですが、タグ付きでなくタグなしのインターフェイスで VLAN を設定する必要があります。図 5.2 に例を示します。

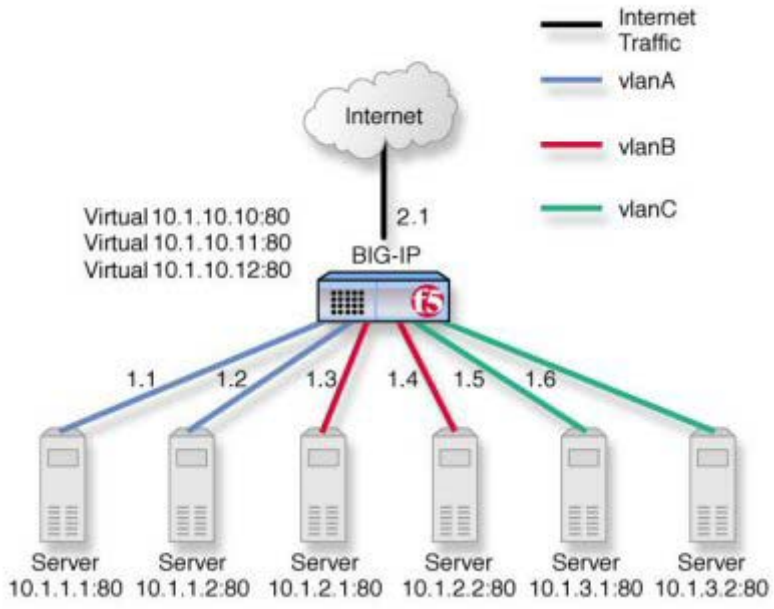

図 5.2 VLAN スイッチングを使用した複数カスタマのホスティング

図 5.2 では、2 つの BIG-IP システムインターフェイスが各 VLAN に割り当てられています。たとえば、インターフェイス 1.1 と 1.2 は、**vlanA** VLAN に割り当てられています。各インターフェイスは、タグなしインターフェイスとして VLAN に割り当てられます。

図 5.1（5-1 ページ）に示すように、最初のシナリオでは追加スイッチが必要ですが、内部ネットワーク上で必要なインターフェイスは 1 つだけです。図 5.2 に示す、第 2 のシナリオでは追加スイッチは不要になりましたが、複数の BIG-IP システムインターフェイスが必要です。

タグなしインターフェイスを持つ VLAN の作成

BIG-IP で複数カスタマの直接ホスティングを設定する場合は、まず、タグなしインターフェイスを追加してVLANを作成してください（タグ付きインターフェイスの詳細については、『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください）。

タグなしインターフェイスを持つ VLAN の作成方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**VLANs**] をクリックします。
   [VLAN] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   VLAN の設定が表示されます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールでは VLAN を作成する権限が与えられていないことを示します。*
3. VLAN の名前とタグ番号を入力します。
   タグ番号を入力しないと、BIG-IP によって自動的に番号が生成されます。図 5.2（5-5 ページ）では、VLAN の名前を **vlanA**、タグ番号を **0001** として一例をあげています。
4. [**Interfaces**]設定では、[**Available**]ボックスから内部ネットワーク上のインターフェイスの名前を選択し、Move ボタン（**>>**）をクリックして、インターフェイスの名前を [**Untagged**] ボックスに移動します。
   [Untagged] ボックスへの移動が完了すると、選択したインターフェイスがタグなしインターフェイスとして VLAN に割り当てられます。図 5.2（5-5 ページ）では、**vlanA** にインターフェイス 1.1 と 1.2 が割り当てられています。**vlanB** にはインターフェイス 1.3 と 1.4 が割り当てられ、**vlanC** にはインターフェイス 1.5 と 1.6 が割り当てられています。
5. [**Finished**] をクリックします。

VLAN を作成してタグなしインターフェイスを割り当てると、「*外部スイッチを使用した複数カスタマのホスティング*」（5-2 ページ）の項で行ったように、プールとバーチャルサーバを作成できます。

6

単純なイントラネット設定

- 単純なイントラネット設定での作業
- 単純なイントラネット設定の作成

単純なイントラネット設定での作業

この章で述べる単純なイントラネット実装は、企業イントラネット内でよく目にします（図 6.1 参照）。この実装では、BIG-IP® は、複数の異なるタイプの接続要求に対してロードバランシングを行います。

- 企業のイントラネット Web サイトへの HTTP 接続。企業イントラネットの Web サイトである **Corporate.main.net** をホストする 2 台の Web サーバを BIG-IP でロードバランスします。
- インターネットコンテンツへの HTTP 接続。インターネットコンテンツへの HTTP 接続は 1 組のキャッシュサーバを使用して処理されますが、このサーバも BIG-IP によりロードバランスされます。
- インターネットへの HTTP 以外の接続。

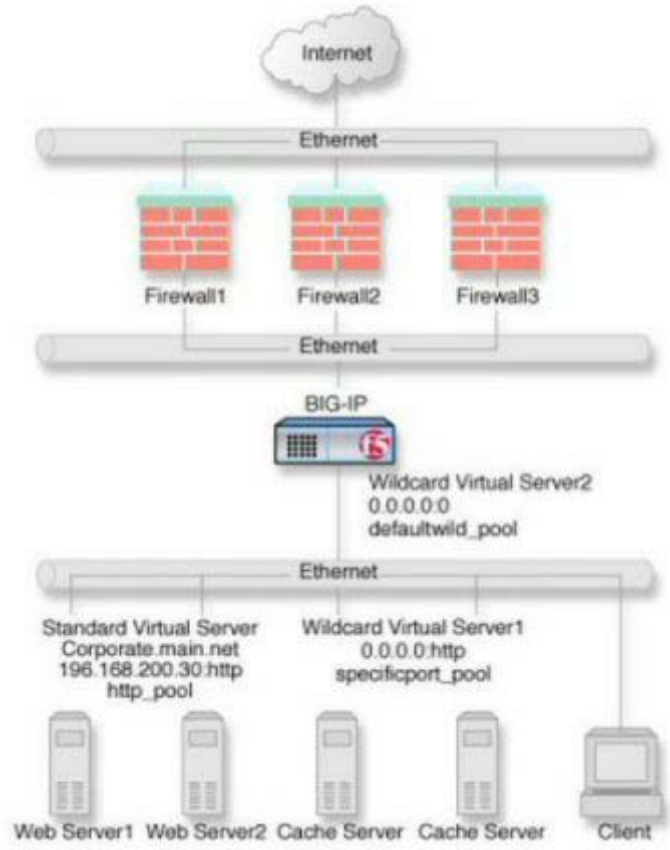

***図 6.1** 単純なイントラネット設定*

図 6.1（6-1 ページ）は、イントラネット以外の接続が、ワイルドカードバーチャルサーバ、つまり **0.0.0.0** の IP アドレスを持つサーバによって処理されていることを示しています。キャッシュサーバへのトラフィックを処理するワイルドカードバーチャルサーバは、ポート固定であり、HTTP 要求に **80** のポートを指定します。このように、イントラネット上の IP アドレスに一致しない HTTP 要求はすべて、

キャッシュサーバにダイレクトされます。HTTP 以外の要求を処理するワイルドカードバーチャルサーバは、デフォルトのワイルドカードサーバです。*デフォルトワイルドカードバーチャルサーバ*は、ポート **0** だけを使用するサーバです。このため、このサーバは、どの標準的なバーチャルサーバにも、どのポート固有のワイルドカードバーチャルサーバにも一致しない発信トラフィックに適合するキャッチオールサーバになっています。

単純なイントラネット設定の作成

この設定を作成するには、次の作業を順番に完了する必要があります。

- **ロードバランシングプールを作成します。**
  ロード バランスするイントラネット サーバ用のプールとキャッシュ サーバ用のプールを作成します。
- **バーチャルサーバを作成します。**
  各プールのバーチャルサーバと HTTP 以外の要求用のバーチャル サーバを作成します。

プールの作成

基本設定では、まず、イントラネットコンテンツサーバ用のプールとインターネットキャッシュサーバ用のプールの 2 つのロードバランシングプールを定義します。

プールの作成方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。
3. [**Name**] ボックスにプールの名前（**http_pool** など）を入力します。
4. 画面の [Resources] 領域で、[**New Members**] 設定を使用してプールメンバを追加します。
   たとえば、図 6.1（6-1 ページ）では、http_pool のプールメンバは **192.168.100.10:80** と **192.168.100.11:80** です。
   specificport_pool のプールメンバは **192.168.100.20:80** と **192.168.100.21:80** です。
5. [**Finished**] をクリックします。

バーチャルサーバの作成

基本設定の次の作業では、**http_pool** と **specificport_pool** をそれぞれ参照するバーチャルサーバを作成します。また、残りのインターネットトラフィック用にフォワーディングバーチャルサーバ（プールなし）も作成してください。

バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注：*[Create] ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスにバーチャルサーバの名前（**vs_http**、**vs_specificport**、**vs_non-http** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
   たとえば、IP アドレス **192.168.200.30:80** を、HTTP トラフィックを処理するバーチャルサーバに割り 当てることができます。キャッシュサーバへの接続のロード バランシングの場合、アドレス **0.0.0.0:80** をバーチャルサーバに割り 当て、このサーバをワイルド カード バーチャルサーバにすることができます。フォワーディング バーチャル サーバを 作成する には、アドレス **0.0.0.0:0** を割り 当てます。
5. [**Service Port**] ボックスに **80** と入力するか、リストから [**HTTP**] を選択します。
6. 画面の [Configuration] 領域で、[**Type**] 設定を探して次の作業を行います。
   a) バーチャルサーバが、イントラネット Web サイトまたはキャッシュサーバへの HTTP トラフィックを処理する場合は、[**Standard**] を選択します。
   b) バーチャルサーバが、HTTP 以外の発信トラフィックを送信する場合は、[**Forwarding (IP)**] を選択します。
7. イントラネット Web サイトへの HTTP 接続を処理するバーチャルサーバを作成している場合は、[**HTTP Profile**] 設定を探して [**http**] を選択します。
8. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、作成しているバーチャルサーバに対応するプールを選択します。
   たとえば、**vs_http** に対しては、プール **http_pool** を選択します。

   注：*フォワーディング（IP）バーチャルサーバを作成している場合は、プールを選択しないでください。*
9. [**Finished**] をクリックします。

7

ISP のロードバランシング

- ISP のロードバランシングの概要
- ISP のロードバランシングの設定
- 発信トラフィックのアドレス変換の設定

ISP のロードバランシングの概要

ネットワークが成長し、ネットワークトラフィックが増大していくと、インターネットへの接続を増強する必要性を感じることがあります。この設定を使用して、既存のネットワークにインターネット接続を追加できます。図 7.1 は、2 つのインターネット接続で構成されたネットワークを示しています。

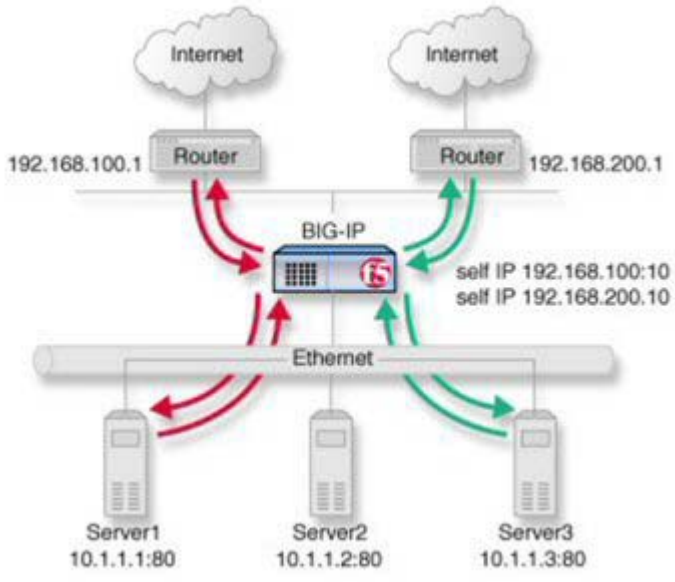

図 7.1 *追加インターネット接続の例*

このような構成の場合は、ルータでネットワークアドレス変換（NAT）を設定する必要があります。ルータで NAT を実行できない場合は、BIG-IP で VLAN SNAT 自動マップ機能を使用します。

ISP のロードバランシングの設定

ISP のロードバランシングを設定するには、BIG-IP 上で次の作業を完了する必要があります。

- **2 つのロードバランシングプールを作成する**
  コンテンツサーバをロードバランスする 1 つのプールを定義します。ルータの内部アドレスをロードバランスする別のプールを定義します。
- **着信および発信トラフィック用のバーチャルサーバを設定する**
  サーバ間での着信接続をロードバランスするバーチャルサーバと、ルータ間での発信接続をロードバランスするバーチャルサーバを設定します。
- **発信トラフィック用の NAT または SNAT 自動マップを設定する**
  要求が送出されたときと同じ ISP を通って応答が到達するように、発信トラフィック用のNATまたはSNAT自動マップを設定します。

追加インターネット接続用プールの作成

まず、コンテンツサーバをロードバランスするプールを 1 つ作成し、ルータをロードバランスするプールを 1 つ作成します。

プールの作成方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、プールの名前（**content_pool**、**router_pool** など）を入力します。
4. 画面の [Resources] 領域で、[**New Members**] 設定を使用してプールメンバを追加します。
   たとえば、図 7.1（7-1 ページ）では、プール **content_pool** のプールメンバは **10.1.1.1:80**、**10.1.1.2:80**、および **10.1.1.3:80** です。プール **router_pool** のプールメンバは **192.168.100.1:0** と **192.168.200.1:0** です。
5. [**Finished**] をクリックします。

追加インターネット接続用バーチャルサーバの作成

プールを作成したら、サーバへの着信接続をロードバランスするバーチャルサーバと、ルータへの発信接続をロードバランスするバーチャルサーバの 2 つのバーチャルサーバを設定します。

着信コンテンツサーバのトラフィック用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_content** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
   たとえば、IP アドレス **172.100.12.20:80** を割り当てることができます。
5. [**Service Port**] ボックスで、ポート番号を入力するか、リストからサービスを選択します。
6. ロードバランスする対象のトラフィックが特定のイプの場合、接続のタイプに一致するプロファイルのタイプを選択します。
   たとえば、ロードバランスする対象のトラフィックが HTTP トラフィックである場合、[**HTTP Profile**] 設定を探して [**http**] を選択します。
7. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、作成しているバーチャルサーバに対応するプールを選択します。
   たとえば、**vs_content** に対しては、プール **content_pool** を選択します。
8. [**Finished**] をクリックします。

ルータの発信トラフィック用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*

3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_routers** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
   たとえば、IP アドレス **0.0.0.0:0** をバーチャルサーバに割り当てて、ワイルドカードバーチャルサーバにすることができます。
5. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、作成しているバーチャルサーバに対応するプールを選択します。
   たとえば、**vs_routers** に対しては、プール **router_pool** を選択します。
6. [**Finished**] をクリックします。

発信トラフィックのアドレス変換の設定

次に、要求が最初に通過したときと同じ ISP を通って応答が到達するように、発信トラフィック用のアドレス変換を設定します。特に、ネットワークアドレス変換（NAT）を実行するようにルータを設定するか、BIG-IP で SNAT 自動マッピングを設定する必要があります。セルフ IP アドレスを、外部 VLAN に割り当てる必要もあります。

◆注

ネットワークアドレス変換を実行するようにルータを設定する手順については、使用しているルータに関するベンダのドキュメントを参照してください。

発信トラフィックのアドレス変換を設定するには、次の作業を行う必要があります。

- IP 固有のセルフ IP アドレスを、2 台のルータの IP ネットワークに対応するように、BIG-IP の外部 VLAN に割り当てます。
- それぞれの外部 VLAN セルフ IP アドレスと内部 VLAN に対して SNAT 自動マップを有効にします。

外部 VLAN 用セルフ IP アドレスの作成方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Self IPs**] をクリックします。
   [Self IP] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   セルフ IP アドレスに対して設定可能な設定が表示されます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではセルフ IP アドレスを作成する権限が与えられていないことを示します。*
3. [**IP Address**] ボックスに、ルータのネットワークに一致するセルフ IP アドレスを入力します。

   注 : *ルータの内部 IP ネットワークアドレスが有効であることを確認します。*
4. [**VLAN**] リストから、[**external**] を選択します。
5. [**Repeat**] をクリックします。
6. 外部 VLAN 用の別のセルフ IP アドレスを作成します。
7. [**Finished**] をクリックします。

内部および外部 VLAN に対して SNAT 自動マップを有効にする方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**SNATs**] をクリックします。
   [SNATs] 画面が開きます。
2. 右上の [**Create**] をクリックします。
   [New SNAT] 画面が開きます。

注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではSNATを作成する権限が与えられていないことを示します。

3. [**Name**] ボックスに、SNAT に一意の名前を入力します。
4. [**Translation**] リストから、[**Automap**] を選択します。
5. [**VLAN Traffic**] リストから、[**Enabled On**] を選択します。[**VLAN List**] 設定が表示されます。
6. [**VLAN List**] 設定では、[**Available**] ボックスから [**internal**] と [**external**] の VLAN 名を選択し、Move ボタン（<<）をクリックして、VLAN 名を [**Selected**] ボックスに移動します。
7. [**Finished**] をクリックします。

8

送信元アドレスアフィニティパーシステンスを使用したHTTPトラフィックのロードバランシング

- 基本的な HTTP のロードバランシングの概要
- 送信元アドレスのアフィニティパーシステンスを使用した HTTP ロードバランシングの設定

基本的な HTTP のロードバランシングの概要

多くのコンピューティング環境で、HTTP トラフィックをインテリジェントに管理するために、BIG-IP が使用されています。HTTP プロファイルと呼ばれる BIG-IP の機能を実装すれば、HTTP トラフィックを容易に制御できます。HTTP プロファイルとは、HTTP トラフィックの動作に影響する一群の設定です。HTTP プロファイルは、BIG-IP で HTTP トラフィックを管理する方法を定義します。

デフォルトのHTTPプロファイルを利用してそのすべてのデフォルト値を使用することも、カスタムの HTTP プロファイルを作成することもできます。カスタム HTTP プロファイルを作成する場合、設定値を修正するだけでなく、サーバ応答のデータ圧縮など、より高度な機能を有効にすることもできます。

HTTP トラフィックの管理に BIG-IP を設定する場合、送信元アドレスのアフィニティパーシステンスとも呼ばれる、シンプルなセッションパーシステンスも実装できます。***送信元アドレスのアフィニティパーシステンス***は、パケットの送信元 IP アドレスにのみ基づいて、同じサーバへセッション要求を転送します。送信元アドレスのアフィニティパーシステンスの実装については、BIG-IP には、ユーザが実装できるデフォルトのパーシステンスプロファイルが用意されています。HTTP の場合と同様、デフォルトのプロファイルを使用することも、カスタムのシンプルパーシステンスプロファイルを作成することもできます。

この章では、デフォルトの HTTP とパーシステンスプロファイルを使用して、基本的な HTTP ロードバランシングシナリオと送信元アドレスのアフィニティパーシステンスの設定方法について説明します。HTTP トラフィックの管理と、送信元アドレスのアフィニティパーシステンスの設定の詳細については、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

送信元アドレスのアフィニティパーシステンスを使用した HTTP ロードバランシングの設定

送信元 IP アドレスに基づいたパーシステンスを使用して、基本的な HTTP ロードバランシングを設定するには、次の作業を行う必要があります。

- **ロードバランシングプールを作成する**
  HTTP 接続をロードバランスするためのプールを作成します。
- **バーチャルサーバを作成する**
  HTTPトラフィックを処理し、プールへ送信するバーチャルサーバを作成します。この実装は、デフォルト の HTTP と送信元アドレスのアフィニティプロファイルを使用して、HTTP ロード バランシングと、セッションパーシステンスを設定するため、これらのプロファイルを設定する必要はありません。作成時に、バーチャルサーバでいくつかの設定を行うだけです。

プールの作成

基本設定では、まず、HTTP 接続をロードバランスするためのロードバランシングプールを作成してください。設定ユーティリティを使用して、このプールを作成します。

HTTPトラフィックのロード バランシング用プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザ ロールではプールを作成する権限が与えられていないことを示します。
3. [**Name**]ボックスにプールの名前(**http_pool**など)を入力します。
4. [**Health Monitors**] 設定では、[**Available**] ボックスから [**http**] を選択し、Move ボタン（<<）をクリックして、モニタ名を [**Active**] ボックスに移動します。
5. [**New Members**] 設定で、次のようにプールメンバを追加します。
   a) [**New Address**] オプションをクリックします。
   b) [**Address**] ボックスに、プール内のサーバの IP アドレスを入力します。
   c) [**Service Port**] ボックスに、**80** と入力するか、[**HTTP**] を選択します。
   d) [**Add**] をクリックします。
   e) プール内のサーバごとに、ステップ b、c、および d を繰り返します。
6. [**Finished**] をクリックします。

バーチャルサーバの作成

基本設定では、次に、HTTP プールを参照するバーチャルサーバを定義してください。設定ユーティリティを使用して、バーチャルサーバを作成します。

HTTP トラフィック用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   ***注**: [Create] ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_http** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] ボックスに **80** と入力するか、リストから [**HTTP**] を選択します。
6. 画面の [Configuration] 領域で、[**HTTP Profile**] 設定を探して [**http**] を選択します。
   これで、デフォルトの HTTP プロファイルがバーチャルサーバに割り当てられます。
7. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、前項で作成した HTTP プールの名前を選択します（たとえば、**http_pool**）。
8. [**Default Persistence Profile**] 設定から、[**source_addr**] を選択します。
   これで、デフォルトの送信元アドレスのアフィニティプロファイルを使用して、シンプルパーシステンスが実装されます。
9. [**Finished**] をクリックします。

9

Cookie パーシステンスを使用した HTTP トラフィックのロードバランシング

- 基本的な HTTP のロードバランシングの概要
- Cookie パーシステンスを使用した HTTP ロードバランシングの設定

基本的な HTTP のロードバランシングの概要

多くのコンピューティング環境で、HTTP トラフィックをインテリジェントに管理するために、BIG-IP が使用されています。HTTP プロファイルと呼ばれる BIG-IP の機能を実装すれば、HTTP トラフィックを容易に制御できます。HTTP プロファイルとは、HTTP トラフィックの動作に影響する一群の設定です。HTTP プロファイルは、システムで HTTP トラフィックを管理する方法を定義します。

デフォルトのHTTPプロファイルを利用してそのすべてのデフォルト値を使用することも、カスタムの HTTP プロファイルを作成することもできます。カスタム HTTP プロファイルを作成する場合、設定値を修正するだけでなく、サーバ応答のデータ圧縮など、より高度な機能を有効にすることもできます。

HTTP トラフィックの管理に BIG-IP を設定する場合、Cookie ベースのセッションパーシステンスも実装できます。***Cookie パーシステンス***は、BIG-IP がクライアントのブラウザに保存している HTTP Cookie に基づいて、セッション要求を同じサーバへ送信します。Cookie パーシステンスを実装するために、BIG-IP には、ユーザが実装できるデフォルトのパーシステンスプロファイルが用意されています。また、カスタムの Cookie パーシステンスプロファイルを作成することもできます。

この章では、デフォルトの TTP プロファイルとカスタムの Cookie パーシステンスプロファイルを使用して、基本的な HTTP ロードバランシングシナリオと Cookie パーシステンスを設定する方法について説明します。HTTP トラフィックの管理と、Cookie パーシステンスの設定の詳細については、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

Cookie パーシステンスを使用した HTTP ロードバランシングの設定

Cookie に基づいたパーシステンスを使用して、基本的な HTTP ロードバランシングを設定するには、次の作業を行う必要があります。

- カスタム Cookie パーシステンスプロファイルを作成する
- ロードバランシングプールを作成する
- HTTP トラフィックを処理し、プールへ送信するバーチャルサーバを作成する

この実装では、既存のデフォルト HTTP プロファイルを使用して、HTTP ロードバランシングを設定するので、HTTP トラフィックの管理にプロファイルを設定する必要は特にありません。設定に必要なプロファイルは、カスタム Cookie パーシステンスプロファイルだけです。

カスタム Cookie パーシステンスプロファイルの作成

Cookie パーシステンスを実装するには、カスタム Cookie パーシステンスプロファイルを作成するのがよい方法です。

カスタム Cookie パーシステンスプロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. メニューバーで [**Persistence**] をクリックします。
   デフォルトのパーシステンスプロファイルのリストが表示されます。
3. 画面右上の [**Create**] をクリックします。
   [New Persistence Profile] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではプロファイルを作成する権限が与えられていないことを示します。
4. [**Name**] ボックスに、プロファイルの名前（**mycookie_profile** など）を入力します。
5. [**Persistence Type**] リストから、[**Cookie**] を選択します。
6. [**Parent Profile**] リストから、[**cookie**] を選択します。
7. [**Cookie Method**] 設定の右端で、[Custom] 選択ボックスをオンにします。
8. [**Cookie Method**] リストから、[**HTTP Cookie Insert**] を選択します。
9. [**Cookie Name**] 設定を無効のままにしておきます。

10. [**Expiration**] 設定で、[**Session Cookie**] チェックボックスをオフにします。
追加設定が表示されます。
11. [**Minutes**] ボックスに **60** と入力します。
12. [**Finished**] をクリックします。

プールの作成

次に、HTTP 接続をロードバランスする対象のロードバランシングプールを作成してください。

HTTPトラフィックのロードバランシング用プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
[Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
[New Pool] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスにプールの名前（**http_pool** など）を入力します。
4. [**Health Monitors**] リストの [**Available**] ボックスから [**http**] を選択し、Move ボタン（<<）をクリックして、モニタ名を [**Active**] ボックスに移動します。
5. [**New Members**] 設定で、次のようにプールメンバを追加します。
   a) [**New Address**] オプションをクリックします。
   b) [**Address**] ボックスに、プール内のサーバの IP アドレスを入力します。
   c) [**Service Port**] ボックスに、**80** と入力するか、[**HTTP**] を選択します。
   d) [**Add**] をクリックします。
   e) プール内のサーバごとに、ステップ b、c、および d を繰り返します。
6. [**Finished**] をクリックします。

バーチャルサーバの作成

基本設定では、次に、HTTP プールを参照するバーチャルサーバを定義してください。

HTTP トラフィック用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_http** など）を入力します。
4. [**Destination**] ボックスで次の作業を行います。
   a) バーチャルサーバのタイプが [**Host**] になっていることを確認します。
   b) [**Address**] ボックスにバーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] ボックスに **80** と入力するか、リストから [**HTTP**] を選択します。
6. 画面の [Configuration] 領域で、[**Protocol**] 設定の値を [**TCP**] のままにしておきます。
7. [**HTTP Profile**] リストから、[**http**] を選択します。
   これで、デフォルトの HTTP プロファイルがバーチャルサーバに割り当てられます。
8. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、前項で作成した HTTP プールの名前を選択します（たとえば、**http_pool**）。
9. [**Default Persistence Profile**] リストから、以前に作成したカスタムクッキープロファイルの名前（**mycookie_profile** など）を選択します。
   これで、カスタム Cookie プロファイルを使用して、Cookie パーステンスが実装されます。
10. [**Finished**] をクリックします。

◆注

パフォーマンス（HTTP）タイプのバーチャルサーバで HTTP Cookie Insert パーシステンスを使用することもできます。

10

HTTP 応答の圧縮

- HTTP データ圧縮の概要
- カスタム HTTP プロファイルの作成
- バーチャルサーバの作成

HTTP データ圧縮の概要

BIG-IP には、対象のサーバからの HTTP 圧縮作業の負荷をシステム側で軽減できるというオプション機能があります。HTTP 圧縮および圧縮ソフトウェア自体の設定に必要なすべての作業は、BIG-IP が集中管理します。

HTTP 圧縮オプションを有効にする主な方法は、HTTP プロファイルの **[Compression]** 設定を **[Enabled]** に設定することです。設定すると、HTTP プロファイルの **[Request-URI]** または **[Content-Type]** 設定で指定した値に一致するすべての応答のHTTPコンテンツがシステム側で圧縮されます。

◆ヒント

*特定の接続に対してHTTP 圧縮を有効にするには、**HTTP:compress enable** コマンドを規定する iRule を作成します。*

BIG-IP の HTTP 圧縮機能を使用する場合、指定した特定のタイプの URI またはファイルを含めることも、除外することもできます。URI またはファイルタイプによっては、すでに圧縮されているものもあるため、この機能は役立ちます。CPU リソースを使用してすでに圧縮済みのデータを圧縮すると、通常はデータの圧縮コストが利点を上回るので、この方法はお勧めしません。除外に指定できる正規表現には、**.*\.pdf**、**.*\.gif**、**.*\.html** などがあります。

HTTP データ圧縮を設定するには、次の作業を行う必要があります。

- カスタム HTTP プロファイルを作成する
- 圧縮した HTTP 応答を処理するバーチャルサーバを作成する

圧縮およびバーチャルサーバの設定に関する詳細な情報については、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

カスタム HTTP プロファイルの作成

BIG-IP で HTTP データ圧縮を設定するには、最初に、カスタム HTTP プロファイルを作成してください。***HTTP プロファイル***は、BIG-IP で HTTP トラフィックを管理する方法を定義します。

カスタム HTTP プロファイルを作成したら、バーチャルサーバを作成し、カスタムプロファイルをそのバーチャルサーバに割り当てます。

カスタム HTTP プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   デフォルトプロファイル **http** を含む、既存の全 HTTP プロファイルのリストが表示されます。
2. 画面右上の [**Create**] をクリックします。
   [New HTTP Profile] 画面が開きます。

   注 :[Create] *ボタンをクリックできない場合は、現在のユーザロールではプロファイルを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、カスタムプロファイルの名前（**http_compress** など）を入力します。
4. [**Parent Profile**] 設定が [**http**] に設定されていることを確認します。
5. 画面の [Settings] 領域で、すべてのデフォルト値をそのまま使用します。
6. Compression 領域で、[**Compression**] 設定に対し、画面の右端の [Custom] ボックスにチェックを入れ、リストから [**Enabled**] をクリックします。
7. HTTP 要求ヘッダに指定された URI に基づいて圧縮を行う場合は、次の作業を行います。
   a) [**URI Compression**] 設定を探し、画面の右端の Select ボックスをクリックして、リストから [**URI List**] をクリックします。
   選択すると、[**URI List**] 設定が表示されます。
   b) 圧縮に含めるまたは圧縮から除外する任意の正規表現を指定します。
   正規表現には、**.*\.pdf**、**.*\.gif**、**.*\.html** などがあります。
8. 応答のコンテンツのタイプに基づいて圧縮を行う場合は、次の作業を行う必要があります。
   a) [**Content Compression**] 設定を探し、画面の右端の Select ボックスをクリックして、リストから [**Content List**] をクリックします。
   選択すると、[**Content List**] 設定が表示されます。
   b) 圧縮に含めるまたは圧縮から除外するコンテンツの値を指定します。
   指定できるコンテンツタイプには、**application/pdf** や **image/**** などがあります。

9. 画面の [Compression] 領域の他のすべての設定については、デフォルトの値をそのまま使用するか、必要に応じて値を設定します。
10. [**Finished**] をクリックします。

バーチャルサーバの作成

HTTP 圧縮の設定の次の作業では、前述の作業で作成したカスタム HTTP プロファイルを参照するバーチャルサーバを定義します。

HTTP 圧縮用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_http_compress** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] ボックスに **80** と入力するか、リストから [**HTTP**] を選択します。
6. 画面の [Configuration] 領域で、[**Protocol**] 設定の値を [**TCP**] のままにしておきます。
7. [**HTTP Profile**] リストから、前項で作成したカスタム HTTP プロファイルを選択します。この例では、**http_compress** になります。
   これで、カスタム HTTP プロファイルがバーチャルサーバに割り当てられます。
8. 画面の [Resources] 領域で、[**Default Pool**] 設定を探してプール名を選択します。
9. [**Default Persistence Profile**] リストから、[**source_addr**] を選択します。
   選択すると、送信元アドレスのアフィニティパーシステンスのデフォルトプロファイルが実装されます。
10. [**Finished**] をクリックします。

カスタム HTTP プロファイルとバーチャルサーバの作成を完了したら、このバーチャルサーバを使用して HTTP トラフィックを送信し、設定をテストできます。BIG-IP によって、カスタムプロファイルで指定した応答が含められたり除外されたりしているか、指定どおりにデータが圧縮されていることかを確認してください。

11

HTTPS のロードバランシングの設定

- HTTPS のロードバランシングの概要
- SSL キーと証明書の作成
- カスタム SSL プロファイルの作成
- プールの作成
- バーチャルサーバの作成

HTTPS のロードバランシングの概要

HTTPS トラフィックをロードバランスする場合、通常は対象の Web サーバで実行する SSL ハンドシェイクを、BIG-IP® で実行するように設定できます。次の 2 つのタイプの SSL 処理を設定できます。次のタイプのいずれか、または両方を設定できます。

- **クライアント側 SSL**
  一般に、BIG-IP の設定では、クライアント側 SSL を有効にします。これにより、システムは、サーバへ送信する前にクライアント要求を復号化し、クライアントに戻す前にサーバ応答を暗号化できるようになります。この場合、キーと証明書のペアを 1 つだけシステムにインストールする必要があります。
- **サーバ側 SSL**
  BIG-IP を設定する別の方法では、サーバ側 SSL を有効にします。これにより、システムは、BIG-IP がターゲット Web サーバに送信する要求を暗号化し、応答を復号化できるようになります。この場合、(クライアント側 SSL でインストールするキーと証明書のペアのほかに) 2 番目のキーと証明書のペアをシステムにインストールする必要があります。

この設定では最初に、必要なキーと証明書のペアをインストールします。

次に、カスタム Client SSL プロファイル、およびオプションでカスタム Server SSL プロファイルを作成できます。***Client SSL*** および ***Server SSL*** プロファイルとは、トラフィックプロファイルであり、完全に SSL カプセル化されたプロトコル（この場合は HTTPS 要求）で送信されるクライアント要求またはサーバ応答を、BIG-IP で処理する方法を定めます。

次に、HTTPS 要求をロードバランスするためのサーバのプールを作成します。

最後に、カスタム Client SSL および Server SSL プロファイルで定めた設定に従って、HTTPS トラフィックを処理するバーチャルサーバを作成する必要があります。

SSL 証明書、SSL プロファイル、ロードバランシングプール、およびバーチャルサーバに関する詳細な情報については、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

SSL キーと証明書の作成

HTTPSトラフィックをロードバランスするには、BIG-IPにインストールする 1 つ以上の SSL キーおよび証明書を作成する必要があります。SSL キーと証明書、次に作成するカスタム Client SSL および Server SSL（オプション）プロファイルを使用すると、通常は対象の Web サーバが実行する SSL ハンドシェイクを、BIG-IP で実行できるようになります。

HTTPS トラフィックを正常に送信できるかテストする場合、信頼された認証局が署名した証明書でなくとも自己署名証明書を使用できます。

自己署名したキーと証明書のペアの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**SSL Certificates**] をクリックします。
   既存の SSL 証明書のリストが表示されます。
2. 画面の右上で [**Create**] をクリックします。
   [New SSL Certificate] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールでは SSL 証明書を作成する権限が与えられていないことを示します。
3. [**Name**] ボックスに、**my_clientside_cert** または **my_serverside_cert** などの証明書の名前を入力します。
4. [**Issuer**] リストから、[**Self**] を選択します。
5. [**Common Name**] ボックスに、後で作成するバーチャルサーバの IP アドレスか、バーチャルサーバの IP アドレスの名前を解決する DNS 名を入力します。
6. [**Organization**] ボックスに、企業名を入力します。
7. [**Division**] ボックスに、部門名を入力します。
8. [**Locality**] ボックスに、所在都市名を入力します。
9. [**State or Province**] ボックスに、所在州名または県名を入力します。
10. [**Country**] リストから、所在国名を選択します。
11. [**E-mail Address**] ボックスに、電子メールアドレスを入力します。
12. [**Challenge Password**] ボックスに、パスワードを入力します。
13. [**Challenge Password**] で入力したパスワードを、[**Confirm Password**] ボックスにもう一度入力します。
14. 画面の [Key Properties] 領域で、[**Size**] リストから、[**1024**] を選択します。
15. [**Finished**] をクリックします。

カスタム SSL プロファイルの作成

BIG-IP で HTTPS ロードバランシングを設定する次の作業は、カスタム SSL プロファイルを作成します。クライアント側 SSL 処理の場合、カスタム Client SSL プロファイルを作成します。サーバ側 SSL 処理の場合、カスタム Server SSL プロファイルを作成します。

SSL プロファイルとは、SSL トラフィックの復号化と暗号化を BIG-IP で実行できるようにする一群の設定です。前述の作業で作成したキーと証明書の名前もカスタム SSL プロファイルで指定するデータです。

カスタム SSL プロファイルを作成した後、ロードバランシングプールを作成してからバーチャルサーバを作成し、カスタムプロファイルをそのバーチャルサーバに割り当てます。

カスタム Client SSL プロファイルを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
2. [SSL] メニューから、[Client] を選択します。
   デフォルトプロファイル **clientssl** を含むすべての既存 Client SSL プロファイルのリストが表示されます。
3. 画面右上の [**Create**] をクリックします。
   [New Client SSL Profiles] 画面が開きます。
4. [**Name**] ボックスに、カスタムプロファイルの名前（**my_clientssl_profile** など）を入力します。
5. [**Parent Profile**] 設定が [**clientssl**] に設定されていることを確認します。
6. [**Certificate**] 設定で、画面の右側の [Custom] ボックスにチェックを入れます。
7. [**Certificate**] リストから、前項で作成した証明書の名前を選択します。
   この例では、**my_clientside_cert.crt** になります。
8. [**Key**] 設定で、画面の右側の [Custom] ボックスにチェックを入れます。
9. [**Key**] リストから、前項で作成したキーの名前を選択します。
   この例では、**my_clientside_cert.key** になります。
10. [**Finished**] をクリックします。

カスタム Server SSL プロファイルを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
2. [SSL] メニューから、[Server] を選択します。
   デフォルトプロファイル **serverssl** を含むすべての既存 Server SSL プロファイルのリストが表示されます。

3. 画面右上の [**Create**] をクリックします。
   [New Server SSL Profiles] 画面が開きます。
4. [**Name**] ボックスに、カスタムプロファイルの名前（**my_serverssl_profile** など）を入力します。
5. [**Parent Profile**]設定が[**serverssl**]に設定されていることを確認します。
6. [**Certificate**] 設定で、画面の右側の [Custom] ボックスにチェックを入れます。
7. [**Certificate**] リストから、前項で作成した証明書の名前を選択します。
   この例では、**my_serverside_cert.crt** になります。
8. [**Key**] 設定で、画面の右側の [Custom] ボックスにチェックを入れます。
9. [**Key**] リストから、前項で作成したキーの名前を選択します。
   この例では、**my_serverside_cert.key** になります。
10. [**Finished**] をクリックします。

プールの作成

次に、HTTP 接続をロードバランスするためのロードバランシングプールを作成してください。プールを作成したら、作成するバーチャルサーバにそのプールを割り当てます。

HTTPトラフィックのロード バランシング用プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、プールの名前（**https_pool** など）を入力します。
4. [**Health Monitors**] 設定では、[**Available**] ボックスから [**http**] を選択し、Move ボタン（**<<**）をクリックして、モニタ名を [**Active**] ボックスに移動します。
5. [**New Members**] 設定で、次のようにプールメンバを追加します。
   a) [**New Address**] オプションをクリックします。
   b) [**Address**] ボックスに、プール内のサーバの IP アドレスを入力します。
   c) [**Service Port**] ボックスに、**80** と入力するか、[**HTTP**] を選択します。
   d) [**Add**] をクリックします。
   e) プール内のサーバごとに、ステップ b、c、および d を繰り返します。
6. [**Finished**] をクリックします。

バーチャルサーバの作成

HTTPS ロードバランシングの設定で、最後に、これまでに作成したカスタムClient SSLプロファイルとロードバランシングプールを参照するバーチャルサーバを定義します。

HTTPS バーチャルサーバを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_clientssl** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] ボックスに **443** と入力するか、リストから [**HTTPS**] を選択します。
6. 画面の [Configuration] 領域で、[**Protocol**] 設定の値を [**TCP**] のままにしておきます。
7. [**Client SSL Profile**]リストから、前項で作成したカスタムClient SSL プロファイルの名前を選択します。この例では、この名前は **my_clientssl_profile** です。
   これで、カスタム Client SSL プロファイルがバーチャルサーバに割り当てられます。
8. カスタムServer SSLプロファイルを作成した場合、[**Server SSL Profile**] リストから、そのプロファイルの名前を選択します。この例では、この名前は **my_serverssl_profile** です。
   これで、カスタム Server SSL プロファイルがバーチャルサーバに割り当てられます。
9. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、前項で作成したプールの名前を選択します。この例では、**https_pool** になります。
10. [**Default Persistence Profile**] リストから、[**source_addr**] を選択します。
    選択すると、送信元アドレスのアフィニティパーシステンスのデフォルトプロファイルが実装されます。
11. [**Finished**] をクリックします。

必要な SSL キーと証明書のペア、1 つまたは 2 つのカスタム SSL プロファイル、ロードバランシングプール、およびバーチャルサーバを作成したら、このバーチャルサーバを通じて HTTPS トラフィックを送信してみることによって設定をテストできます。

12

データ圧縮を使用した HTTPS のロードバランシングの設定

- 圧縮を使用した HTTPS のロードバランシングの概要
- SSL キーと証明書の作成
- カスタム Client SSL プロファイルの作成
- 圧縮用のカスタム HTTP プロファイルの作成
- プールの作成
- バーチャルサーバの作成

圧縮を使用した HTTPS のロードバランシングの概要

HTTPS トラフィックのデータ圧縮を有効にして、HTTPS トラフィックをロードバランスする場合、通常は対象の Web サーバで実行する SSL ハンドシェイクを、BIG-IP で実行するように設定できます。一般に、BIG-IP の設定では、サーバへ送信する前にクライアント要求を復号化し、クライアントに戻す前にサーバ応答を暗号化するように設定します。

一般に、SSL ハンドシェイクを実行する（したがって HTTPS トラフィックを処理する）ように BIG-IP を設定するには、まず、SSL キーと証明書を要求して、BIG-IP にインストールします。BIG-IP は、キーと証明書のペアを使用して、クライアント要求をサーバに送信する前に復号化するサーバとして機能し、サーバ応答をクライアントに戻す前に暗号化します。

キーと証明書のペアをインストールすると、カスタム Client SSL プロファイルを作成できます。***Client SSL プロファイル***とは 1 種のトラフィックプロファイルであり、完全に SSL カプセル化されたプロトコル（この場合は HTTPS 要求）で送信されるクライアント要求を、BIG-IP で処理する方法を定めます。

次に、カスタム HTTP プロファイルを作成して、BIG-IP でデータ圧縮を有効にします。有効にしたら、HTTPS 要求をロードバランスするためのサーバのプールを作成する必要があります。

最後に、カスタム Client SSL プロファイルで定めた設定に従って、HTTPS トラフィックを処理するバーチャルサーバを作成する必要があります。

SSL 証明書、SSL プロファイル、ロードバランシングプール、およびバーチャルサーバに関する詳細な情報については、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

◆注

*サーバ側 SSL 処理の設定については、第 11 章「**HTTPS のロードバランシングの設定**」を参照してください。*

SSL キーと証明書の作成

HTTPS トラフィックをロードバランスし、圧縮を有効にするには、BIG-IP にインストールする SSL キーと証明書を作成する必要があります。SSL キーと証明書、次に作成するカスタム Client SSL プロファイルを使用すると、通常は対象の Web サーバが実行する SSL ハンドシェイクを、BIG-IP で実行できるようになります。

HTTPS トラフィックを正常に送信できるかテストする場合、信頼された認証局が署名した証明書でなくとも自己署名証明書を使用できます。

自己署名したキーと証明書のペアの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**SSL Certificates**] をクリックします。
   既存の SSL 証明書のリストが表示されます。
2. 画面の右上で [**Create**] をクリックします。
   [New SSL Certificate] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールでは SSL 証明書を作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、証明書の名前（**my_cert** など）を入力します。
4. [**Issuer**] リストから、[**Self**] を選択します。
5. [**Common Name**] ボックスに、この章で後から作成するバーチャルサーバの IP アドレスか、バーチャルサーバの IP アドレスを名前解決する DNS 名を入力します。
6. [**Organization**] ボックスに、企業名を入力します。
7. [**Division**] ボックスに、部門名を入力します。
8. [**Locality**] ボックスに、所在都市名を入力します。
9. [**State or Province**] ボックスに、所在州名または県名を入力します。
10. [**Country**] リストから、所在国名を選択します。
11. [**E-mail Address**] ボックスに、電子メールアドレスを入力します。
12. [**Challenge Password**] ボックスに、パスワードを入力します。
13. [**Challenge Password**] で入力したパスワードを、[**Confirm Password**] ボックスにもう一度入力します。
14. 画面の [Key Properties] 領域で、[**Size**] リストから、[**1024**] を選択します。
15. [**Finished**] をクリックします。

カスタム Client SSL プロファイルの作成

圧縮を使用した HTTPS のロードバランシングの設定では、次に、カスタム Client SSL プロファイルを作成してください。***Client SSL プロファイル***とは、BIG-IP でクライアント側の SSL トラフィックの復号化と暗号化を実行させるための一群の設定です。前項で作成したキーと証明書の名前も Client SSL プロファイルで指定するデータです。

カスタム Client SSL プロファイルを作成した後、ロードバランシングプール、バーチャルサーバの順に作成し、そのバーチャルサーバにカスタムプロファイルを割り当てます。

カスタム Client SSL プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. [SSL] メニューから、[Client SSL] を選択します。
   デフォルトプロファイル **clientssl** を含むすべての既存 Client SSL プロファイルのリストが表示されます。
3. 画面右上の [**Create**] をクリックします。
   [New Client SSL Profiles] 画面が開きます。

   注 :[Create] *ボタンをクリックできない場合は、現在のユーザロールではプロファイルを作成する権限が与えられていないことを示します。*
4. [**Name**] ボックスに、カスタムプロファイルの名前（**clientssl_profile** など）を入力します。
5. [**Parent Profile**] 設定が [**clientssl**] に設定されていることを確認します。
6. [**Certificate**] 設定で、画面の右側の [Custom] ボックスにチェックを入れます。
7. [**Certificate**] リストから、前項で作成した証明書の名前を選択します。
   この例では、**my_cert.crt** になります。
8. [**Key**] 設定で、画面の右側の [Custom] ボックスにチェックを入れます。
9. [**Key**] リストから、前述の作業で作成したキーの名前を選択します。
   この例では、**my_cert.key** になります。
10. [**Finished**] をクリックします。

圧縮用のカスタム HTTP プロファイルの作成

BIG-IP で HTTP データ圧縮を有効にするには、カスタム HTTP プロファイルを作成する必要があります。***HTTP プロファイル***は、BIG-IP で HTTP トラフィックを管理する方法を定義します。

カスタム HTTP プロファイルを作成したら、ロードバランシングプールを作成します。続いて、バーチャルサーバを作成し、カスタム HTTP プロファイルをそのバーチャルサーバに割り当てます。

圧縮用カスタム HTTP プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   デフォルトプロファイル **http** を含む、既存の全 HTTP プロファイルのリストが表示されます。
2. 画面右上の [**Create**] をクリックします。
   [New HTTP Profile] 画面が開きます。

   注 :[Create] *ボタンをクリックできない場合は、現在のユーザロールではプロファイルを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、カスタムプロファイルの名前（**http_compress** など）を入力します。
4. [**Parent Profile**] 設定が [**http**] に設定されていることを確認します。
5. 画面の [Settings] 領域で、すべてのデフォルト値をそのまま使用します。
6. [**Compression**] 設定に対し、画面の右端の Select ボックスをオンにして、リストから [**Enabled**] を選択します。
7. HTTP 要求ヘッダに指定された URI に基づいて圧縮を行う場合は、次の作業を行います。
   a) [**URI Compression**] 設定を探し、画面の右端の Select ボックスをオンにして、リストから [**URI List**] をクリックします。
   選択すると、[**URI List**] 設定が表示されます。
   b) 圧縮に含めるまたは圧縮から除外する任意の正規表現を指定します。
   正規表現には、**.*\.pdf**、**.*\.gif**、**.*\.html** などがあります。
8. 応答のコンテンツのタイプに基づいて圧縮を行う場合は、次の作業を行う必要があります。
   a) [**Content Compression**] 設定を探し、画面の右端の Select ボックスをオンにして、リストから [**Content List**] をクリックします。
   選択すると、[**Content List**] 設定が表示されます。
   b) 圧縮に含めるまたは圧縮から除外するコンテンツの値を指定します。
   指定できるコンテンツタイプには、**application/pdf** や **image/**** などがあります。

9. 画面の [Compression] 領域の他のすべての設定については、デフォルトの値をそのまま使用するか、必要に応じて値を設定します。
10. [**Finished**] をクリックします。

プールの作成

次に、HTTP 接続をロードバランスするためのロードバランシングプールを作成してください。プールを作成したら、作成するバーチャルサーバにそのプールを割り当てます。

HTTPトラフィックのロード バランシング用プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、プールの名前（**https_pool** など）を入力します。
4. [**Health Monitors**] 設定では、[**Available**] ボックスから [**http**] を選択し、Move ボタン（<<）をクリックして、モニタ名を [**Active**] ボックスに移動します。
5. [Resource] 領域の [**New Members**] 設定で、次のようにプールメンバを追加します。
   a) [**New Address**] オプションをクリックします。
   b) [**Address**] ボックスに、プール内のサーバの IP アドレスを入力します。
   c) [**Service Port**] ボックスに、**80** と入力するか、[**HTTP**] を選択します。
   d) [**Add**] をクリックします。
   e) プール内のサーバごとに、ステップ b、c、および d を繰り返します。
6. [**Finished**] をクリックします。

バーチャルサーバの作成

HTTPS ロードバランシングの設定で、最後に、これまでに作成したカスタムClient SSLプロファイルとロードバランシングプールを参照するバーチャルサーバを定義します。

HTTPS 圧縮用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_clientssl** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] ボックスに **443** と入力するか、リストから [**HTTPS**] を選択します。
6. 画面の [Configuration] 領域で、[**Protocol**] 設定の値を [**TCP**] のままにしておきます。
7. [**HTTP Profile**] リストから、作成した HTTP プロファイルの名前を選択します。
   この例では、**http_compress** になります。
8. [**Client SSL Profile**]リストから、前項で作成したカスタムClient SSL プロファイルを選択します。この例では、**clientssl_profile** になります。
   これで、カスタム Client SSL プロファイルがバーチャルサーバに割り当てられます。
9. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、前項で作成したプールの名前を選択します。この例では、**https_pool** になります。
10. [**Default Persistence Profile**] リストから、[**source_addr**] を選択します。
    選択すると、送信元アドレスのアフィニティパーシステンスのデフォルトプロファイルが実装されます。
11. [**Finished**] をクリックします。

これで、バーチャルサーバを使用して HTTPS トラフィックを送信し、設定をテストできます。BIG-IP によって、カスタム HTTP プロファイルで指定した応答が含められたり除外されたりしているか、指定どおりにデータが圧縮されていることかを確認してください。

13

HTTP トラフィック用の RAM キャッシュの使用

- HTTP RAM キャッシュの概要
- カスタム HTTP プロファイルの作成
- バーチャルサーバの作成

HTTP RAM キャッシュの概要

BIG-IP®には、HTTP RAMキャッシュという機能が用意されています。***RAM キャッシュ***とは、BIG-IP のランダムアクセスメモリ（RAM）に保存された HTTP オブジェクトのキャッシュであり、バックエンドサーバでの負荷を軽減するために以降の接続で再利用できます。

RAM キャッシュを使用する場合

RAM キャッシュ機能を使用すると、バックエンドサーバへのトラフィック負荷を軽減できます。サイトのオブジェクトに対する需要が高い場合、サイトに大量のスタティックコンテンツがある場合、またはサイトのオブジェクトが圧縮されている場合に、この機能は役立ちます。

- **高需要オブジェクト**
  この機能は、特定のコンテンツに対する需要が高い時間帯があるサイトに役立ちます。RAM キャッシュを設定すると、コンテンツサーバは、1 有効期間に 1 度、BIG-IP にコンテンツを配信するだけでよくなります。
- **スタティックコンテンツ**
  サイトが大量のスタティックコンテンツ（CSS、JavaScript、イメージ、ロゴなど）で構成されている場合にも、この機能が役立ちます。
- **コンテンツ圧縮**
  圧縮可能なデータの場合、RAM キャッシュは、圧縮データに対応できるクライアントのデータを保存できます。RAMキャッシュは、BIG-IP の圧縮機能と一緒に使用すると、BIG-IP とコンテンツサーバの負荷を軽減します。

キャッシュ可能な項目

RAM キャッシュ機能は、RFC 2616、*Hypertext Transfer Protocol -- HTTP/1.1* に記述されているキャッシュ仕様に完全に準拠しています。したがって、RAM キャッシュは、次のコンテンツタイプをキャッシュするように設定できます。

- **200**、**203**、**206**、**300**、**301**、および **410** 応答
- GET メソッドへの応答（デフォルト）
- URI Include リストに指定された、または iRule で指定された URI の他の HTTP メソッド
- **User-Agent** 値および **Accept-Encoding** 値に基づくコンテンツ。RAM キャッシュは、**Vary** ヘッダにさまざまなコンテンツを格納します。

RAM キャッシュ機能を使用するには、次の作業を行う必要があります。

- カスタム HTTP プロファイルを作成する
- バーチャルサーバを作成する

RAM Cache 機能の設定に関する詳細な情報については、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

カスタム HTTP プロファイルの作成

BIG-IP で HTTP RAM キャッシュ機能を設定するには、最初に、カスタム HTTP プロファイルを作成してください。***HTTP プロファイル***は、BIG-IP で HTTP トラフィックを管理する方法を定義します。

カスタム HTTP プロファイルを作成したら、バーチャルサーバを作成し、カスタムプロファイルをそのバーチャルサーバに割り当てます。

カスタム HTTP プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Profiles**] をクリックします。
   デフォルトプロファイル **http** を含む、既存の全 HTTP プロファイルのリストが表示されます。
2. 画面右上の [**Create**] をクリックします。
   [New HTTP Profile] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではプロファイルを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、カスタムプロファイルの名前（**http_ramcache** など）を入力します。
4. [**Parent Profile**] 設定が [**http**] に設定されていることを確認します。
5. 画面の [Settings] 領域で、すべてのデフォルト値をそのまま使用します。
6. 画面の [RAM Cache] 領域までスクロールダウンします。
7. [**RAM Cache**] 設定では、画面の右端の Select ボックスをクリックして、[**RAM Cache**] リストから [**Enabled**] をクリックします。
8. 画面の [RAM Cache] 領域の他のすべての設定については、デフォルトの値をそのまま使用するか、必要に応じて値を設定します。
9. [**Finished**] をクリックします。

バーチャルサーバの作成

RAMキャッシュ機能の設定では、次に、前項で作成したカスタムHTTPプロファイルを参照するバーチャルサーバを定義してください。

HTTP RAM キャッシュ用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_http_compress** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] ボックスに **80** と入力するか、リストから [**HTTP**] を選択します。
6. 画面の [Configuration] 領域で、[**Protocol**] 設定の値を [**TCP**] のままにしておきます。
7. [**HTTP Profile**] リストから、前項で作成したカスタム HTTP プロファイルを選択します。この例では、**http_ramcache** になります。
   これで、カスタム HTTP プロファイルがバーチャルサーバに割り当てられます。
8. 画面の [Resources] 領域で、[**Default Pool**] 設定を探してプール名を選択します。
9. [**Default Persistence Profile**] リストから、[**source_addr**] を選択します。
   選択すると、送信元アドレスのアフィニティパーシステンスのデフォルトプロファイルが実装されます。
10. [**Finished**] をクリックします。

14

パッシブモードの FTP トラフィックのロードバランシング

- FTP のロードバランシングの概要
- カスタム FTP モニタの作成
- プールの作成
- バーチャルサーバの作成

FTP のロードバランシングの概要

パッシブモードの FTP トラフィックをロードバランスするように、BIG-IP を設定できます。この設定を行うには、次の作業を行います。

- カスタム FTP ヘルスモニタを作成する
- FTP トラフィックのロードバランシング用プールを作成する
- FTP トラフィックの処理用のバーチャルサーバを作成する

バーチャルサーバを作成するときに、デフォルトの FTP プロファイルを使用するように設定できます。***FTP プロファイル***によって、BIG-IP で FTP トラフィックを処理する方法を定義します。

この章では、デフォルト FTP プロファイルを使用して上記のオブジェクトを作成する方法について説明します。FTP トラフィックの管理の詳細については、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

カスタム FTP モニタの作成

FTP サーバのファイルを監視するカスタム FTP モニタを作成できます。

カスタム FTP モニタの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Monitors**] をクリックします。
   既存のヘルスモニタとパフォーマンスモニタのリストが表示されます。
2. 画面の右上で [**Create**] をクリックします。
   [New Monitor] 画面が開きます。
3. [**Name**] ボックスに、カスタムモニタの名前（**my_ftp_monitor** など）を入力します。
4. [**Type**] リストから、[**FTP**] を選択します。
   これで、その他の FTP モニタ設定が表示されます。
5. [**User Name**] ボックスに、FTP サーバのログオン名を入力します。
6. [**Password**] ボックスに、ログオン名のパスワードを入力します。
7. [**Path/Filename**] ボックスに、監視するファイルのパスと名前を入力します。
8. [**Mode**] 設定が [**Passive**] に設定されていることを確認します。
9. 他のすべての設定については、デフォルト値をそのまま使用します。
10. [**Finished**] をクリックします。

カスタム FTP モニタの作成を完了したら、FTP トラフィック用のロードバランシングプールを作成します。

プールの作成

パッシブモードの FTP トラフィックをロードバランスするには、ロードバランシングプールを作成します。プールを作成するときに、前述の作業で作成したカスタム FTP モニタを割り当てます。

プールを作成したら、作成するバーチャルサーバにそのプールを割り当てます。

FTP トラフィックのロードバランシング用プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、プールの名前（**ftp_pool** など）を入力します。
4. [**Health Monitors**] 設定では、[**Available**] ボックスから **my_ftp_monitor** などのカスタム FTP モニタの名前を選択し、Move ボタン（<<）をクリックして、モニタ名を [**Active**] ボックスに移動します。
5. [**Priority Group Activation**] が [**Disabled**] に設定されていることを確認します。
6. [**New Members**] 設定で、次のようにプールメンバを追加します。
   a) [**New Address**] オプションをクリックします。
   b) [**Address**] ボックスに、プール内のサーバの IP アドレスを入力します。
   c) [**Service Port**] リストから、[**FTP**] を選択します。
   d) [**Add**] をクリックします。
   e) プール内のサーバごとに、ステップ b、c、および d を繰り返します。
7. [**Finished**] をクリックします。

バーチャルサーバの作成

基本設定の次の作業では、FTP プロファイルと FTP プールを参照するバーチャルサーバを定義します。

FTP トラフィック用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_ftp** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] リストから、[**FTP**] を選択します。
6. [**FTP Profile**] リストから [**ftp**] を選択します。
   これで、デフォルト FTP プロファイルがバーチャルサーバに割り当てられます。
7. 画面の Resources 領域で、[**Default Pool**] 設定を探し、前述の作業で作成した FTP プールの名前を選択します（たとえば、**ftp_pool**）。
8. [**Default Persistence Profile**] 設定から、[**source_addr**] を選択します。
   これで、デフォルトの送信元アドレスのアフィニティプロファイルを使用して、シンプルパーシステンスが実装されます。
9. [**Finished**] をクリックします。

15

レートシェイピングを使用したパッシブモードの FTPトラフィックのロードバランシング

- レートシェイピングを使用した FTP のロードバランシングの概要
- カスタム FTP モニタの作成
- プールの作成
- レートクラスの作成
- バーチャルサーバの作成

レートシェイピングを使用した FTP のロード バランシングの概要

レートシェイピングを使用してパッシブモードの FTP トラフィックをロードバランスするように、BIG-IP を設定できます。この設定を行うには、次の作業を行います。

- カスタム FTP ヘルスモニタを作成する
- FTP トラフィックのロードバランシング用プールを作成する
- レートクラスを作成する
- FTP トラフィックの処理用のバーチャルサーバを作成する

バーチャルサーバを作成するときに、デフォルトの FTP プロファイルを使用するように設定できます。***FTP プロファイル***によって、BIG-IP で FTP トラフィックを処理する方法を定義します。

この章では、デフォルト FTP プロファイルを使用して上記のオブジェクトを作成する方法について説明します。FTP トラフィックの管理の詳細については、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

BIG-IP では、レートシェイピング機能はオプションです。したがって、レートシェイピングを使用してパッシブ FTP トラフィックのロードバランシングを制御するには、レートシェイピング機能用のライセンスを購入しておく必要があります。

カスタム FTP モニタの作成

FTP サーバのファイルを監視するカスタム FTP モニタを作成できます。

カスタム FTP モニタの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Monitors**] をクリックします。
   既存のヘルスモニタとパフォーマンスモニタのリストが表示されます。
2. 画面の右上で [**Create**] をクリックします。
   [New Monitor] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではカスタムモニタを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、カスタムモニタの名前（**my_ftp_monitor** など）を入力します。
4. [**Type**] リストから、[**FTP**] を選択します。
   これで、その他の FTP モニタ設定が表示されます。
5. [**User Name**] ボックスに、FTP サーバのログオン名を入力します。
6. [**Password**] ボックスに、ログオン名のパスワードを入力します。
7. [**Path/Filename**] ボックスに、監視するファイルのパスと名前を入力します。
8. [**Mode**] 設定が [**Passive**] に設定されていることを確認します。
9. 他のすべての設定については、デフォルト値をそのまま使用します。
10. [**Finished**] をクリックします。

カスタム FTP モニタの作成を完了したら、FTP トラフィック用のロードバランシングプールを作成します。

プールの作成

パッシブモードの FTP トラフィックをロードバランスするには、ロードバランシングプールを作成します。プールを作成するときに、前述の作業で作成したカスタム FTP モニタを割り当てます。

レートシェイピングを使用した FTP トラフィックのロードバランシング用プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、プールの名前（**ftp_pool** など）を入力します。
4. [**Health Monitors**] 設定では、[**Available**] ボックスから **my_ftp_monitor** などのカスタム FTP モニタの名前を選択し、Move ボタン（<<）をクリックして、モニタ名を [**Active**] ボックスに移動します。
5. [**Priority Group Activation**] 設定が [**Disabled**] に設定されていることを確認します。
6. [**New Members**] 設定で、次のようにプールメンバを追加します。
   a) [**New Address**] オプションをクリックします。
   b) [**Address**] ボックスに、プール内のサーバの IP アドレスを入力します。
   c) [**Service Port**] リストから、[**FTP**] を選択します。
   d) [**Add**] をクリックします。
   e) プール内のサーバごとに、ステップ b、c、および d を繰り返します。
7. [**Finished**] をクリックします。

プールの作成後、次の作業で、作成するバーチャルサーバにそのプールを割り当てます。

レートクラスの作成

レートシェイピングを実装するには、レートクラスを作成します。レートクラスを作成することにより、レートシェイピングにより制御されるパッシブモードの FTP トラフィックをロードバランスできます。

◆注

レートシェイピングは BIG-IP のオプション機能です。レートシェイピングを実装する前に、この機能を使用するためのライセンスを取得していることを確認してください。

レートクラスの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Rate Shaping**] をクリックします。
   [Rate Shaping] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Rate Class] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではレートクラスを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、レートクラスの名前（**ftp_rateclass** など）を入力します。
4. [**Base Rate**] ボックスで、**1** と入力して、リストから [**Mbps**] を選択します。
5. [**Ceiling Rate**] ボックスに、**10** と入力して、リストから [**Mbps**] を選択します。
6. [**Burst Rate**] ボックスに **10000** と入力します。
7. 他のすべての設定については、デフォルト値をそのまま使用します。
8. [**Finished**] をクリックします。

バーチャルサーバの作成

基本設定の次の作業では、FTP プロファイルと FTP プールを参照するバーチャルサーバを定義します。

レートシェイピングを使用したFTPトラフィック用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_ftp** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] リストから、[**FTP**] を選択します。
6. [**FTP Profile**] リストから、[**ftp**] を選択します。
   これで、デフォルト FTP プロファイルがバーチャルサーバに割り当てられます。
7. [**Rate Class**] リストから、前項で作成したレートクラスの名前を選択します（たとえば、**ftp_rateclass**）。
8. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、前項で作成したFTPプールの名前を選択します（たとえば、**ftp_pool**）。
9. [**Default Persistence Profile**] 設定から、[**source_addr**] を選択します。
   これで、デフォルトの送信元アドレスのアフィニティプロファイルを使用して、シンプルパーシステンスが実装されます。
10. [**Finished**] をクリックします。

16

単一 IP ネットワークトポロジのセットアップ

- 単一 IP ネットワークトポロジの概要
- 単一 IP ネットワークトポロジ用のプールの作成
- バーチャルサーバの作成
- デフォルトルートの定義
- クライアント SNAT の設定

単一 IP ネットワークトポロジの概要

BIG-IP で使用できるそのほかの構成として、単一 IP ネットワークトポロジがあります。単一 IP ネットワークトポロジは、次の 2 つの点で通常の 2 ネットワーク構成とは異なります。

- 物理的なネットワークは 1 つしかないため、この構成では、BIG-IP 上に複数のインターフェイスを必要としません。
- クライアントがロードバランシングプールのネットワーク上のサーバに接続できるように、SNAT をクライアントに割り当てる必要があります。

図 16.1 は、単一インターフェイス構成を示しています。

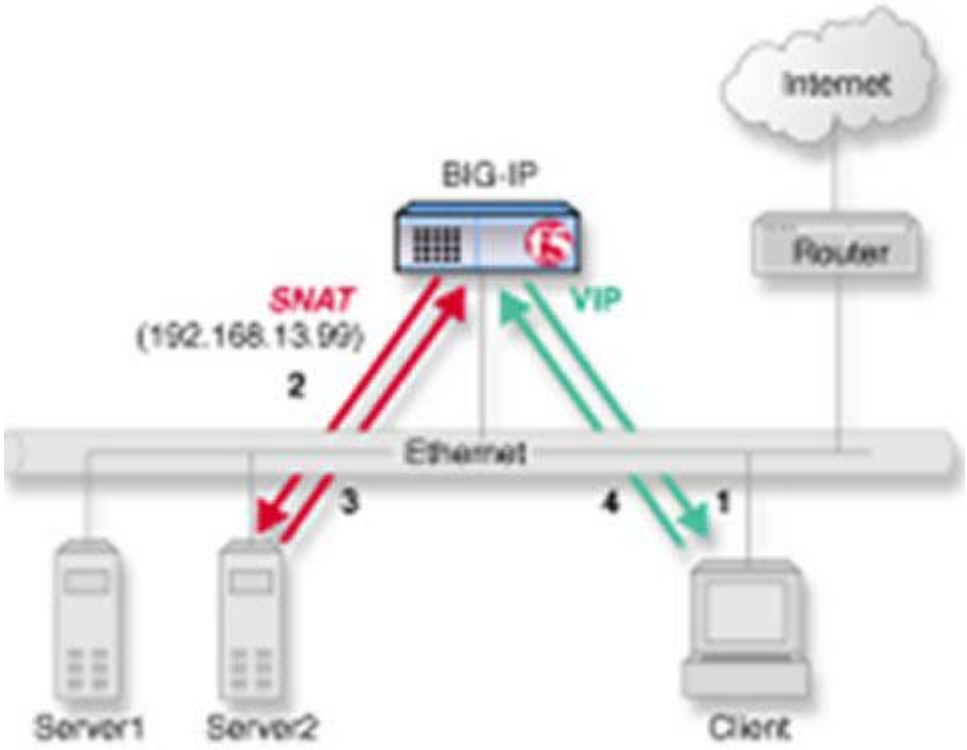

***図 16.1** 単一インターフェイストポロジの例*

この構成をセットアップするには、BIG-IP で次の作業を完了する必要があります。

- コンテンツサーバのロードバランシングプールを作成する
- コンテンツサーバプールへのトラフィックをロードバランスするバーチャルサーバを作成する
- 外部 VLAN のデフォルトルートを定義する
- クライアントの SNAT を設定する

単一 IP ネットワークトポロジ用のプールの作成

この実装のセットアップでは、最初に、ロードバランスするコンテンツサーバを含むプールを作成してください。プールを作成する前に、プールのすべてのコンテンツサーバが、VLAN **external** のネットワーク内にあることを確認してください。

プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Configuration**] リストから、[**Advanced**] を選択します。
4. [**Name**] ボックスに、プールの名前（**server_pool** など）を入力します。
5. [**Health Monitors**] 設定では、[**Available**] ボックスから [**http**] を選択し、Move ボタン（<<）をクリックして、モニタ名を [**Active**] ボックスに移動します。
6. [**Allow SNAT**] 設定では、値が **Yes** になっていることを確認します。
7. 画面の [Configuration] 領域の残りの設定については、デフォルト値をそのまま使用します。
8. 画面の [Resources] 領域では、[**Load Balancing Method**] 設定と [**Priority Group Activation**]設定のデフォルト値を使用します。
9. [**New Members**] 設定で、次のようにプールメンバを追加します。
   a) [**New Address**] オプションをクリックします。
   b) [**Address**] ボックスに、プール内のサーバの IP アドレスを入力します。
   c) [**Service Port**] ボックスに、**80** と入力するか、[**HTTP**] を選択します。
   d) [**Add**] をクリックします。
   e) プール内のサーバごとに、ステップ b、c、および d を繰り返します。
10. [**Finished**] をクリックします。

バーチャルサーバの作成

この実装のセットアップでは、次に、ロードバランスするサーバのプールを参照するバーチャルサーバを作成します。バーチャルサーバが参照するプールは、前項で作成したプールです。

バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_one_ip** など）を入力します。
4. [**Destination**] 設定で、次の作業を行います。

   a) バーチャルサーバのタイプが [**Host**] になっていることを確認します。

   b) [**Address**] ボックスにバーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] ボックスに **80** と入力するか、リストから [**HTTP**] を選択します。
6. 画面の [Configuration] 領域で、[**Protocol**] 設定の値を [**TCP**] のままにしておきます。
7. [**HTTP Profile**] リストから、[**http**] を選択します。
   これで、デフォルトの HTTP プロファイルがバーチャルサーバに割り当てられます。
8. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、前項で作成したプールの名前を選択します（この例では **server_pool** になります）。
9. [**Finished**] をクリックします。

デフォルトルートの定義

単一 IP ネットワークのロードバランシングを実装するには、さらに、VLAN **external** のデフォルトルートを定義する必要があります。

デフォルトルートの定義方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Routes**] をクリックします。
   [Routes] 画面が開きます。
2. 画面の右上で [**Add**] をクリックします。
   [New Route] 画面が開きます。

   注：*[Add] ボタンをクリックできない場合は、現在のユーザロールではルートを追加する権限が与えられていないことを示します。*
3. [**Type**] 設定では、[**Default Gateway**] に設定されていることを確認します。
   これで、[**Destination**] 設定と [**Netmask**] 設定が無効になります。
4. [**Resource**] 設定で、次の作業を行います。

   a) 左側のリストから、[**Use VLAN**] を選択します。

   b) 右側のリストから、[**external**] を選択します。
5. [**Finished**] をクリックします。

◆注

*ルートドメイン **0** (デフォルトルートドメイン) 以外のルートドメインのデフォルトルートを定義する場合、手順が若干異なります。詳細については、『**TMOS™ Management Guide for BIG-IP® Systems**』を参照してください。*

クライアント SNAT の設定

最後に、クライアントから開始した接続を処理するように、BIG-IP を設定します。パケットの送信元アドレスを、BIG-IP 上に置かれた SNAT 外部アドレスに変更するように、SNAT を定義する必要があります。定義しないと、戻りパケットの送信元アドレスがコンテンツサーバの IP アドレスになっている場合、クライアントは、コンテンツサーバではなくバーチャルサーバの IP アドレスにパケットを送信したため、このパケットを認識しません。

SNAT を定義しない場合、送信元アドレスをサーバアドレスからバーチャルサーバのアドレスに戻す機会を BIG-IP に与えずに、サーバはパケットを直接クライアントへ戻します。この場合、クライアントはこのパケットを認識不可として拒否します。

クライアント SNAT の設定方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**SNATs**] をクリックします。
   [SNATs] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New SNAT] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではSNATを作成する権限が与えられていないことを示します。
3. [**Name**] ボックスに、SNAT の名前（**snat_one_ip** など）を入力します。
4. [**Translation**] ボックスに、変換 IP アドレスとして使用する IP アドレスを入力します。
5. [**Origin**] リストから、[**Address List**] を選択します。
   これで、追加の設定が表示されます。
6. [**Address List**] 設定で、次の作業を行います。
   a) [**Type**] 設定では、[**Host**] が有効になっていることを確認します。
   b) [**Address**] ボックスに、クライアントの IP アドレスを入力します。
   c) [**Add**] をクリックします。
   d) 変換アドレスを割り当てるクライアントごとに、このプロセスを繰り返します。
7. [**VLAN Traffic**] リストから、[**Enabled on**] を選択します。
8. [**VLAN List**] 設定では、[**Available**] ボックスから [**external**] を選択し、Move ボタン（<<）をクリックして、VLAN 名を [**Active**] ボックスに移動します。
9. [**Finished**] をクリックします。

17

タグ付き VLAN でのリンクアグリゲーションの使用

- タグ付き VLAN インターフェイスでのリンクアグリゲーションの概要
- 2 ネットワーク構成でアグリゲートしたタグ付きインターフェイストポロジの使用
- 1 ネットワーク構成でのアグリゲートしたタグ付きインターフェイストポロジの使用

タグ付きVLANインターフェイスでのリンクアグリゲーションの概要

アグリゲートした 2 インターフェイスロードバランシングトポロジで、BIG-IP を使用できます。リンクアグリゲーションとは、複数のリンクを結合し、1 つのリンクとして処理することで帯域幅を増加させるプロセスのことです。リンクアグリゲーションは、トランクを作成すると発生します。*トランク*は、2 つ以上のインターフェイスとケーブルを組み合わせ、1 つのリンクとして構成したものです。

この章の例では、アグリゲートした 2 つのタグ付きインターフェイスを含むトランクを示します。*タグ付きインターフェイス*は、複数の VLAN のトラフィック処理用に設定されたインターフェイスです。VLAN タグにより、特定の VLAN を識別して、トラフィックがこの特定 VLAN を通過できるようにします。複数の VLAN のトラフィックが単一のトランクを通過するためには、この同一のトランクを各 VLAN に割り当てる必要があります。

例では、1.1 と 1.2 という 2 つのインターフェイスを含むトランク（**trunk1**）を作成し、trunk1 をタグ付きインターフェイスとして VLAN external と VLAN internal の両方に割り当てます。その結果、BIG-IP とベンダースイッチの間を通過する着信および送信トラフィックは、いずれかのインターフェイスを利用できるようになります。たとえば、VLAN external に向かうトラフィックは、インターフェイス 1.1 または 1.2 のいずれかを通過することになります。

2 つのインターフェイスを 1 つのトランクにアグリゲートして単一のリンクを作成することにより、次の利点が得られます。

- 個々のネットワークインターフェイスカード（NIC）の帯域幅が累積的に増大します。
- 一方のリンクがダウンしても、他方のリンクが単独でトラフィックを処理できます。

この章の例では、2 つのネットワーク構成と単一のネットワーク構成という 2 とおりの構成において、リンクアグリゲーションの使用方法を示します。

2ネットワーク構成でアグリゲートしたタグ付きインターフェイストポロジの使用

図 17.1 に、**外部** VLAN（VLAN external）に接続された 1 つのネットワークと、**内部** VLAN（VLAN internal）に接続された別のネットワークで構成される 2-IP ネットワークのトポロジを示します。

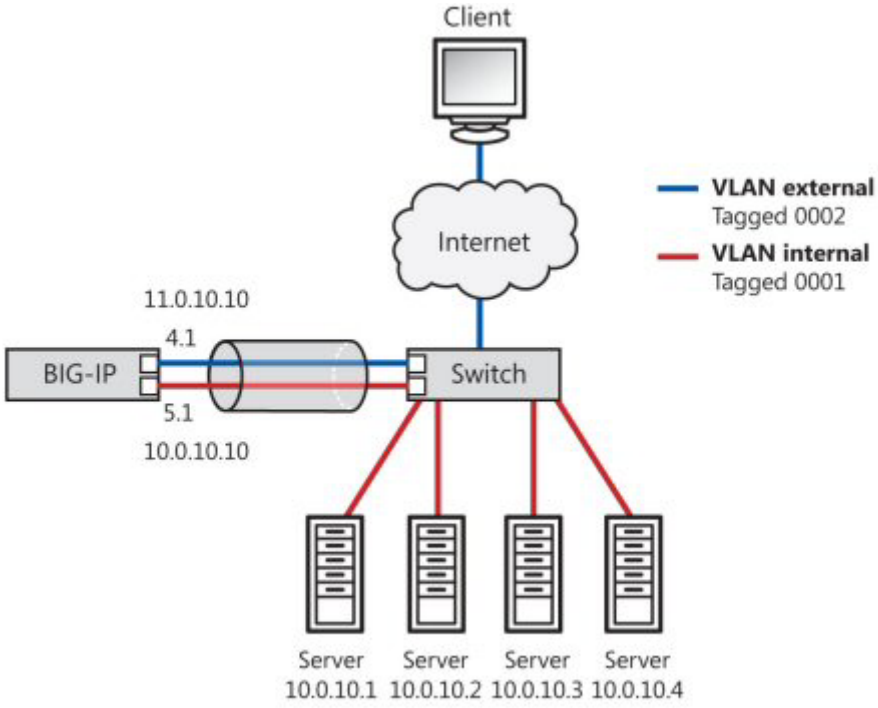

図 17.1 *2 つの IP ネットワークでのアグリゲートした 2 インターフェイスロードバランシング設定の例*

BIG-IP で 2 ネットワーク実装を設定するには、次の作業を完了する必要があります。

- リンクをアグリゲートするトランクを作成する
- このトランクをタグ付きインターフェイスとして VLAN **internal** と VLAN **external** に追加する
- ロードバランスする Web サーバのプールを作成する
- Web サーバをロードバランスするバーチャルサーバを作成する

◆注

*この例では、デフォルトの**内部** VLAN 設定および**外部** VLAN 設定を使用していること、各 VLAN 上のセルフ IP アドレスは、BIG-IP と同じ IP ネットワーク上にあることを前提としています。*

リンクのアグリゲート

この実装の最初の作業は、リンクのアグリゲートです。リンクをアグリゲートするには、トランクを作成して、このトランクにメンバとしてインターフェイスを割り当ててから、LACP（Link Aggregation Control Protocol）を有効にします。

リンクをアグリゲートする方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Trunks**] をクリックします。
   [Trunks] 画面が開きます。
2. 画面の右上で [**Create**] をクリックします。
   [New Trunk] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではトランクを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、トランクの名前（**trunk1** など）を入力します。
4. [**Interfaces**]設定で、[**Available**]ボックスを探してインターフェイスを選択します。

   注 : *番号が最も小さいインターフェイスは、制御用（参照用）のインターフェイスです。*
5. Move ボタンを使用して、インターフェイス番号を [**Members**] ボックスに移動します。
6. トランクメンバとして含めるすべてのインターフェイスに対して、ステップ 5 を繰り返します。
7. [**LACP**] 設定でボックスのチェックをオンにします。
   これで、ダイナミックリンクアグリゲーションが有効になります。
8. [**Finished**] をクリックします。

VLAN へのトランクの割り当て

トランクをアグリゲートしたら、このトランクをタグ付きインターフェイスとして VLAN に割り当てます。

◆警告

この作業は管理インターフェイスから実行してください。管理インターフェイス以外から実行すると、BIG-IP から切断されます。

既存の VLAN へのタグ付きインターフェイスの追加方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**VLANs**] をクリックします。
   [VLAN] 画面が開きます。

2. Name カラムで、VLAN 名 **internal** をクリックします。
この VLAN のプロパティが表示されます。
3. [**Interfaces**] 設定で、[**Available**] ボックスを探して、前の手順で作成したトランクの名前を選択します。
4. Move ボタンをクリックして、このトランク名を [**Tagged**] ボックスに移動します。
これで、選択したインターフェイスがタグ付きインターフェイスとして VLAN に割り当てられます。
5. [**Update**] をクリックします。
6. 既存の VLAN のリストに戻ります。
7. VLAN **external** に対して、手順 2 ～ 5 を繰り返します。
8. [**Update**] をクリックします。

ロードバランスする Web サーバのプールの作成

BIG-IP 用のネットワーク環境を作成してから、ロードバランスする Web サーバのプールを作成します。

プールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
[Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
[New Pool] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。
3. [**Name**] ボックスに、プールの名前（**myweb_pool** など）を入力します。
4. [**New Members**] 設定で、次のようにプールメンバを追加します。
   a) [**New Address**] オプションをクリックします。
   b) [**Address**] ボックスに、プール内の Web サーバの IP アドレスを入力します。
   c) [**Service Port**] リストからサービスを選択します。
   d) [**Add**] をクリックします。
   e) プール内のサーバごとに、ステップ b、c、および d を繰り返します。
5. [**Finished**] をクリックします。

Web サーバをロードバランスするバーチャルサーバの作成

ロードバランスする Web サーバのプールを作成してから、バーチャルサーバを作成します。

バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   ***注**: **[Create]** ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_myweb** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。図 17.1（17-2 ページ）を例にとると、**10.0.10.30** がバーチャルサーバの IP アドレスになります。
5. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、前項で作成したプールの名前を選択します（たとえば、**myweb_pool**）。
6. [**Default Persistence Profile**] 設定から、[**source_addr**] を選択します。
   これで、デフォルトの送信元アドレスのアフィニティプロファイルを使用して、シンプルパーシステンスが実装されます。
7. [**Finished**] をクリックします。

1 ネットワーク構成でのアグリゲートしたタグ付きインターフェイストポロジの使用

図 17.2 は、単一 IP ネットワークトポロジを示しています。1 ネットワークトポロジは 2 ネットワークトポロジとほとんど同じですが、1 ネットワーク実装では VLAN **internal** と VLAN **external** が同じ内部ネットワークにある点が異なります。したがって、パケットを直接交換できるように、2 つの VLAN をグループ化する必要があります。

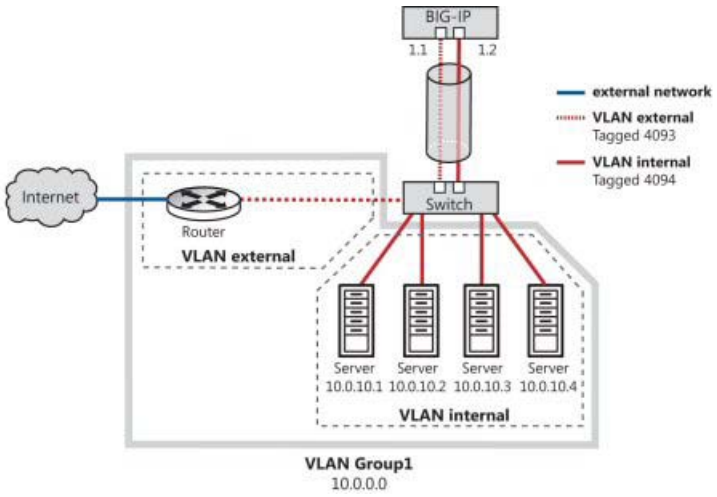

***図 17.2** 単一 IP ネットワークでのアグリゲートした 2 インターフェイスロードバランシング設定の例*

1 ネットワークトポロジは、内部および外部 VLAN をグループ化するという 1 つのステップが追加されますが、2 ネットワークトポロジとまったく同じ方法で設定できます（今回は、バーチャルサーバアドレスがサーバと同じネットワークに属しています）。したがって、BIG-IP でこの実装を設定するには、次の作業を完了する必要があります。

- タグ付きインターフェイス、ロードバランシングプール、バーチャルサーバ、トランクを、2 ネットワーク構成の場合と同じように設定する詳細については、「*2 ネットワーク構成でアグリゲートしたタグ付きインターフェイストポロジの使用*」（17-2 ページ）を参照してください。
- 内部 VLAN と外部 VLAN からセルフ IP アドレスを削除する
- 内部 VLAN と外部 VLAN を 1 つの VLAN グループにまとめる
- VLAN グループにセルフ IP アドレスを割り当てる

VLAN からのセルフ IP アドレスの削除

VLAN グループを作成する前に、個々の VLAN からセルフ IP アドレスを削除する必要があります。VLAN グループを作成し、ルーティング用に VLAN グループのセルフ IP アドレスを作成します。作成後は、VLAN ごとのセルフ IP アドレスは不要になります。

◆警告

この作業は管理インターフェイスから実行してください。管理インターフェイス以外から実行すると、BIG-IP から切断されます。

デフォルト VLAN からのセルフ IP アドレスの削除方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Self IPs**] をクリックします。
   [Self IPs] 画面が開きます。
2. IP Address カラムと VLANs カラムを使用して、内部 VLAN と外部 VLAN のセルフ IP アドレスを探します。
3. 削除するセルフ IP アドレスの左側の [Select] ボックスをオンにします。
4. [**Delete**] をクリックします。
   確認画面が表示されます。
   注 : [Delete] ボタンをクリックできない場合は、現在のユーザロールではセルフ IP アドレスを削除する権限が与えられていないことを示します。
5. もう一度、[**Delete**] をクリックします。

VLAN グループの作成

内部 VLAN と外部 VLAN を含めた VLAN グループを作成します。VLAN グループ内の VLAN が受信したパケットは、他方の VLAN にもコピーされます。これでトラフィックは、同じ IP ネットワーク上の BIG-IP を通過できるようになります。

◆ヒント

VLAN 名を使用できるところであればどこでも VLAN グループ名を使用できます。

VLAN グループを作成するには

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**VLANs**] をクリックします。
   [VLANs] 画面が開きます。
2. [VLAN Groups] メニューから、[List] を選択します。
   [VLAN Groups] 画面が開きます。
3. 画面右上の [**Create**] をクリックします。
   [New VLAN Group] 画面が開きます。

注 : [Create] ボタンをクリックできない場合は、現在のユーザロールでは VLAN グループを作成する権限が与えられていないことを示します。

4. [**Name**] ボックスに、グループ名 **myvlangroup** を入力します。
5. [**VLANs**]設定では、Moveボタンを使用して、**内部**と**外部**VLAN名を、[**Available**] ボックスから [**Members**] ボックスへ移動します。
6. [**Finished**] をクリックします。

VLAN グループ用のセルフ IP アドレスの作成

VLAN グループを作成したら、VLAN グループ用のセルフ IP アドレスを作成します。VLAN グループ用のセルフ IP アドレスは、ネットワークに宛てられたパケットにルートを与えます。BIG-IP を使用した場合、IP ネットワークへのパスは VLAN です。ただし、この例で使用した VLAN グループ機能では、IP ネットワーク **10.0.0.0** へのパスは、実際には複数の VLAN を経由します。IP ルータは、ネットワークへの物理ルートを 1 つしか指定できないので、ルーティング衝突が発生します。BIG-IP でのセルフ IP アドレス機能は、セルフ IP アドレスを VLAN グループ上に設定することにより、ルーティング衝突を解消できます。

VLAN グループ用セルフ IP の作成方法

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Self IPs**] をクリックします。
   [Self IPs] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではセルフIP アドレスを作成する権限が与えられていないことを示します。
3. [**IP Address**] ボックスに、VLAN グループ用のセルフ IP を入力します。
4. [**Netmask**] ボックスに、セルフ IP アドレスのネットマスクを入力します。
5. [**VLAN**] 設定で、リストから名前の [**myvlangroup**] を選択します。
6. [**Finished**] をクリックします。

18

パケットフィルタリングのセットアップ

- パケットフィルタリングの概要
- パケットフィルタリングの設定

パケットフィルタリングの概要

パケットフィルタは、ユーザが指定した基準に基づいて、BIG-IP システムインターフェイスで特定のパケットを許可するか拒否するかを指定して、ネットワークのセキュリティを強化します。パケットフィルタは、着信トラフィックに対してアクセスポリシーを実施します。これは着信トラフィックにのみ適用されます。

パケットフィルタルールを作成し、パケットフィルタリングを実装します。***パケットフィルタルール***の主な目的は、パケットフィルタリング時に BIG-IP で使用する基準を定義することです。パケットフィルタルールで指定できる基準には、たとえば次のものがあります。

- パケットの送信元 IP アドレス
- パケットの宛先 IP アドレス
- パケットの宛先ポート

式の中で、パケットフィルタルールの適用基準を指定します。パケットフィルタルールを作成するときには、設定ユーティリティを利用して式を作成することも（この場合、事前定義されたリストから基準を選択するだけです）、**tcpdump** ユーティリティの構文を使用して、ユーザ自身の式テキストを作成することもできます。**tcpdump** ユーティリティの詳細については、オンラインマニュアルの **tcpdump** コマンドに関するページを参照してください。

◆注

パケットフィルタルールには iRules™ との関連性はありません。

また、作成したすべてのパケットフィルタルールに適用されるグローバルパケットフィルタリングも設定できます。以降の項では、グローバルパケットフィルタリングオプションの設定方法と、個々のパケットフィルタルールの作成と管理方法について説明します。

いくつかの基本 IP ルーティングをセットアップし、パケットフィルタリングを設定すると、内部 VLAN 上の特定のホストから内部 VLAN のセルフ IP アドレスに接続できるようになります。また、これらのホストは HTTP、HTTPS、DNS、FTP、SSH などの一般的なインターネットサービスも使用できます。内部 VLAN 内のほかのすべてのホストからのトラフィックは拒否されます。

この実装を設定するには、次の作業を行う必要があります。

- SNAT を作成する
- ルータのプールを作成する（ゲート ウェイプールとも呼ばれます。）
- フォワーディングバーチャルサーバを作成する
- パケットフィルタルールを作成する

パケットフィルタリングの設定

この項では、完全なパケットフィルタリングを実行するのに必要な作業について説明します。

SNAT の作成

パケットフィルタリングの実装では、最初に、SNAT を作成します。

SNAT を作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**SNATs**] をクリックします。
   [SNATs] 画面が開きます。
2. 右上の [**Create**] をクリックします。
   [New SNAT] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではSNATを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、SNAT に一意の名前を入力します。
4. [**Translation**] リストから、[**Automap**] を選択します。
5. [**VLAN Traffic**] リストから、[**Enabled On**] を選択します。
   [**VLAN List**] 設定が表示されます。
6. [**VLAN List**] 設定では、[**Available**] ボックスから [**internal**] と [**external**] を選択し、Move ボタン (**<<**) をクリックして、VLAN 名を [**Selected**] ボックスに移動します。
7. [**Finished**] をクリックします。

ゲートウェイプールの作成

次に、ゲートウェイプールとも呼ばれる、ルータのプールを定義します。

ゲートウェイプールを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、プールの名前（**gateway_pool** など）を入力します。

4. 画面の [Resources] 領域で、[**New Members**] 設定を使用してプールメンバを追加します。
   追加するメンバはルータの IP アドレスです。
5. [**Finished**] をクリックします。

フォワーディングバーチャルサーバを作成する

次に、プール **gateway_pool** を参照するフォワーディングバーチャルサーバを作成します。

バーチャルサーバを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_packetfilter** など）を入力します。
4. [**Destination**] 設定で、次の作業を行います。

   a) [**Type**] に [**Network**] を選択します。

   b) [**Address**] ボックスに、IP アドレス **0.0.0.0** を入力します。

   c) [**Mask**] ボックスに、ネットマスク **0.0.0.0** を入力します。
5. [**Service Port**] リストから、[***All Ports**] を選択します。
6. 画面の [Configuration] 領域で、[**Type**] 設定を探して [**Forwarding (IP)**] を選択します。
7. [**Protocol**] リストから、[***All Protocols**] を選択します。
8. [**VLAN Traffic**] リストから、[**Enabled On**] を選択します。
9. [**VLAN List**] 設定では、[**Available**] ボックスから [**internal**] を選択し、Move ボタン（**<<**）をクリックして、VLAN 名を [**Selected**] ボックスに移動します。
10. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、以前に作成したプールの名前（**gateway_pool**）を選択します。
11. [**Finished**] をクリックします。

パケットフィルタルールの作成

パケットフィルタリングの実装では、最後に、パケットフィルタルールを作成します。パケットフィルタルールは、iRule とは異なることに注意してください。

パケットフィルタルールを作成するには

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Packet Filters**] をクリックします。
   パケットフィルタリングを有効または無効にする設定が表示されます。
2. [**Packet Filtering**] リストから、[**Enabled**] を選択します。
   その他の設定が表示されます。
3. [**Unhandled Packet Action**] リストから、[**Accept**] を選択します。
4. [**Update**] をクリックします。
5. メニューバーで [**Rules**] をクリックします。
   既存のパケットフィルタルールがある場合は、そのリストが表示されます。
6. 画面の右上で [**Create**] をクリックします。
   [New Packet Filter Rule] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではパケットフィルタルールを作成する権限が与えられていないことを示します。*
7. [**Name**] ボックスに、パケットフィルタ名（**pf_internal** など）を入力します。
8. [**Order**] リストから、[**First**] を選択します。
9. [**Action**] リストから、[**Reject**] を選択します。
10. [**Apply to VLAN**] リストから、[**internal**] を選択します。
11. [**Logging**] リストから、[**Enabled**] を選択します。
12. [**Filter Expression Method**] リストから、[**Enter Expression Text**] を選択します。
    これで、[**Filter Expression**] テキストボックスが表示されます。
13. テキストボックスに、式を入力します。たとえば、次のようになります。

    ```
    not dst port 80 and not dst port 443 and not dst port 53
    and no dst port 22 and not dst port 20 and not dst port
    21 and not dst host <internal self IP address>
    ```

    注 : <internal self IP address> *は、VLAN* ***internal*** *の実際のセルフ IP アドレスに置き換えてください。また、式の作成に関する概要については、****tcpdump*** *マニュアルページも参照してください。*
14. [**Finished**] をクリックします。

19

ヘルスモニタとパフォーマンスモニタの実装

- ヘルスモニタとパフォーマンスモニタの概要
- カスタムモニタの作成
- プールの作成
- バーチャルサーバの作成

ヘルスモニタとパフォーマンスモニタの概要

ロードバランシングプールのメンバである特定のノードまたはサーバの健全性またはパフォーマンスを監視するように、BIG-IP を設定できます。***モニタ***は、プールメンバとノードの接続を確認します。モニタはヘルスモニタとパフォーマンスモニタのどちらかであり、プール、プールメンバ、またはノードの状態を稼働時に一定間隔でチェックするように設計されています。チェック中のプールメンバまたはノードが指定のタイムアウト時間内に応答しない場合や、プールメンバまたはノードの状態がパフォーマンスの低下を示している場合に、BIG-IP は別のプールメンバまたはノードにトラフィックをリダイレクトします。

モニタは、BIG-IP の一部として組み込まれている場合もありますが、ユーザが作成する場合もあります。BIG-IP に用意されているモニタは、***設定済みモニタ***と呼ばれます。ユーザが作成するモニタは、***カスタムモニタ***と呼ばれます。

モニタの設定や使用の前に、モニタタイプ、モニタの設定、およびモニタの実装に関する基本概念を理解しておくことをお勧めします。

- **モニタタイプ**
  設定済みモニタであってもカスタムモニタであっても、すべてのモニタは特定のタイプに属します。各タイプのモニタは、特定のプロトコル、サービス、またはアプリケーションの状態をチェックします。たとえば、モニタタイプの 1 つが HTTP です。HTTP タイプのモニタでは、プール、プールメンバまたはノードの HTTP サービスのアベイラビリティを監視できます。WMI のモニタタイプは、Windows Management Instrumentation（WMI）ソフトウェアを実行しているプール、プールメンバ、またはノードのパフォーマンスを監視します。ICMP タイプのモニタは、単にノードの状態が **up** であるか **down** であるかを判断します。
- **モニタの設定**
  どのモニタにも値が設定されています。この設定と値は、モニタタイプにより異なります。場合によっては、BIG-IP がデフォルト値を割り当てます。たとえば、図 19.1 は、ICMP タイプのモニタの設定とデフォルト値を示しています。

```
Name my_icmp
Type ICMP
Interval 5
Timeout 16
Transparent No
Alias Address * All Addresses
```

図 19.1 *デフォルト値が設定されたモニタの例*

ヘルスモニタを実装するには、次の作業を完了します。

- カスタムモニタを作成するか、設定済みモニタを使用するかを決定する
- トラフィックのロードバランシング用のプールを作成し、モニタをそのプールに割り当てる
- トラフィック処理用のバーチャルサーバを作成する

この章では、これらのオブジェクトの作成方法について説明します。

◆注

*RealNetworks® RealServer サーバ、または Windows Management Instrumentation（WMI）を備えた Windows® サーバのパフォーマンスを監視する場合は、まず、特別なプラグインファイルを BIG-IP にダウンロードします。詳細については、『**BIG-IP® Local Traffic Management 設定ガイド**』を参照してください。*

カスタムモニタの作成

ノード、サーバ、またはサーバのプールの監視には、設定済みモニタを使用することも、カスタムモニタを作成することもできます。次の手順では、カスタムモニタを作成する方法を説明します。設定済みモニタを使用する場合は、この手順をスキップして、次の「*プールの作成*」（19-4 ページ）の項に進んでください。

カスタムモニタの作成方法

1. ナビゲーションペインの [Main] タブで、**[Local Traffic]** を展開して **[Monitors]** をクリックします。
   既存のヘルスモニタとパフォーマンスモニタのリストが表示されます。
2. 画面の右上で **[Create]** をクリックします。
   [New Monitor] 画面が開きます。

   ***注：[Create]** ボタンをクリックできない場合は、現在のユーザロールではモニタを作成する権限が与えられていないことを示します。*
3. **[Name]** ボックスに、カスタムモニタの名前を入力します。
   たとえば、カスタム HTTP モニタを作成する場合、名前の **my_http_monitor** を割り当てます。
4. **[Type]** リストから、作成するモニタタイプを選択します。
   その他のモニタ設定が表示されます。

   注：各モニタタイプの詳細については、『Configuration Guide for BIG-IP® Local Traffic Management』を参照してください。
5. 必要に応じてモニタ設定の値を変更します。
6. **[Finished]** をクリックします。

カスタムモニタの作成を完了したら、ロードバランシングプールを作成し、そのプールにモニタ名を割り当てます。

プールの作成

トラフィックをロードバランスするプールを作成するときに、前項で作成したカスタムモニタをロードバランシングプールに割り当てます。プールを作成したら、次の項で、作成するバーチャルサーバにそのプールを割り当てます。

プールへのモニタの割り当て

モニタを割り当てるには、プールを作成して、そのプール自体にモニタを割り当てる方法があります。モニタをプールに割り当てると、プールのすべてのメンバがそのモニタを継承します。プールに割り当てるモニタの継承から、1 つまたは複数のプールメンバを除外する場合は、「*モニタからのプールメンバの除外*」（19-5 ページ）を参照してください。

プールを作成してモニタを割り当てる方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスにプールの名前（**http_pool** など）を入力します。
4. [**Health Monitors**] 設定では、[**Available**] ボックスから **my_http_monitor** などのカスタムモニタの名前を選択し、Move ボタン（**<<**）をクリックして、モニタ名を [**Active**] ボックスに移動します。
5. [Resources] セクションで、[**Load Balancing Method**] 設定が [**Round Robin**] に設定されていることを確認します。
6. [**Priority Group Activation**] 設定が [**Disabled**] に設定されていることを確認します。
7. [**New Members**] 設定で、次のようにプールメンバを追加します。

   a) [**New Address**] オプションをクリックします。

   b) [**Address**] ボックスに、プール内のサーバの IP アドレスを入力します。

   c) [**Service Port**] リストから、[**FTP**] を選択します。

   d) [**Add**] をクリックします。

   e) プール内のサーバごとに、ステップ b、c、および d を繰り返します。
8. [**Finished**] をクリックします。

モニタからのプールメンバの除外

プールを作成した後、次の 2 つの内のいずれかの方法で、モニタの継承からプールメンバを除外できます。

- プールメンバからのモニタの削除
- プールメンバへの別のモニタの割り当て

プールメンバからのモニタの削除は、ロードバランシングプール内の（全サーバではなく）一部のサーバを監視する場合に役に立ちます。プールに割り当てたモニタの継承からプールメンバを除外する場合、プールメンバに別のモニタを割り当てるというオプションがあります。この場合、他のプールメンバはそのまま、プール自体に割り当てたモニタにより監視されます。

プールに割り当てたモニタからプールメンバを除外するには、まず、「*プールを作成してモニタを割り当てる方法*」（19-4 ページ）に従う必要があります。さらに、次の手順のいずれかを使用します。

プールメンバからのモニタの削除方法

1. ナビゲーションペインの [Main] タブで、**[Local Traffic]** を展開して **[Pools]** をクリックします。
   既存のプールのリストが表示されます。
2. **Name** カラムで、「*プールへのモニタの割り当て*」（19-4 ページ）で作成したプールの名前をクリックします。
3. メニューバーで **[Members]** をクリックします。
   画面の [Current Members] 領域に、プールのメンバが一覧表示されます。
4. Members カラムで、モニタを削除するプールメンバのアドレスをクリックします。
   そのプールメンバのプロパティが表示されます。
5. **[Configuration]** リストから、**[Advanced]** を選択します。
   これで、**[Health Monitors]** 設定が表示されます。
6. **[Health Monitors]** リストから、**[None]** を選択します。
7. **[Update]** をクリックします。

プールメンバに一意のモニタを割り当てる方法

1. ナビゲーションペインの [Main] タブで、**[Local Traffic]** を展開して **[Pools]** をクリックします。
   既存のプールのリストが表示されます。
2. Name カラムで、「*プールへのモニタの割り当て*」（19-4 ページ）で作成したプールの名前をクリックします。
3. メニューバーで **[Members]** をクリックします。
   画面の [Current Members] 領域に、プールのメンバが一覧表示されます。
4. Members カラムで、ユニークなモニタを割り当てるプールメンバのアドレスをクリックします。
   そのプールメンバのプロパティが表示されます。

5. [**Configuration**] リストから、[**Advanced**] を選択します。
これで、[**Health Monitors**] 設定が表示されます。
6. [**Health Monitors**] リストから、[**Member Specific**] を選択します。
7. [**Update**] をクリックします。

バーチャルサーバの作成

基本設定の最後の作業では、「*プールの作成*」（19-4 ページ）で作成したプールを参照するバーチャルサーバを定義します。設定ユーティリティを使用して、バーチャルサーバを作成します。

バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
[Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
[New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_httppool** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] リストからサービスを選択します。
6. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、作成したプールの名前（**http_pool** など）を選択します。
7. [**Finished**] をクリックします。

20

IPv6 ノードへのトラフィックのロードバランシング

- radvd サービスの設定
- IPv4 と IPv6 間のロードバランシングの設定

radvd サービスの設定

IPv4 と IPv6 間のゲートウェイとして機能するように BIG-IP を設定するには、最初に、オプションの **radvd** サービスを設定します。ICMPv6 ルーティングアドバイザリメッセージを送出し、ICMPv6 ルート要請メッセージに応答するように、**radvd** サービスを設定します。

この作業を実行すると、BIG-IP により下流ノードの自動設定がサポートされるようになります。また、下流ノードは、BIG-IP がそのルータであることを自動的に検出します。

これらの機能が実行されるように **radvd** サービスを設定すると、最終的に、ネットワークのグローバルアドレスプレフィックスが内部 VLAN でアドバタイズされます。BIG-IP システムサービスの詳細については、『***TMOS*™ *Management Guide for BIG-IP*® *Systems***』を参照してください。

radvd サービスの設定方法

1. シリアルコンソールまたは BIG-IP システム管理インターフェイスの IP アドレスを使用して、BIG-IP のオペレーティングシステムのプロンプトにアクセスします。
2. ファイル **/etc/radvd.conf.example** を、新しいファイル **/etc/radvd.conf** にコピーします。
3. **nano** または **vi** テキストエディタを使用して、ファイル **/etc/radvd.conf** を開きます。
4. ファイル内の例を使用して、ネットワークのグローバルアドレスプレフィックスのアドバタイズ設定を作成します。

   ***注 : prefix** オプションは、ユーザのネットワークに適したアドレスに置き換えてください。*
5. **/etc/radvd.conf** ファイルを保存して、エディタを終了します。
6. 次のように、**radvd** サービスを起動します。

   ```
   bigstart startup radvd
   ```
7. IPv6 ノードがこのプレフィックスに対してそのアドレスを自動設定していることを確認します。
8. HTTP サービス用 IPv6 ノードのアドレスに注意してください。これらのアドレスは、このプロセスの次のステップで IPv4 と IPv6 間のロードバランシングを設定する際に必要になります。

IPv4 と IPv6 間のロードバランシングの設定

IPv4 と IPv6 間のロードバランシングを設定する場合、IPv6 ノードへトラフィックをロードバランスするためのプールを作成し、次に、アプリケーショントラフィックを処理する IPv4 バーチャルサーバを作成します。

これらの作業の詳細については、設定ユーティリティの [Help] タブまたは『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

IPv6 ノードのプールの作成

IPv4 と IPv6 ロードバランシングの設定では、まず、IPv6 ノードへの接続をロードバランスするためのプールを作成します。設定ユーティリティを使用して、このプールを作成します。

IPv6 ノードのプールの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。
3. [**Name**] ボックスに、プールの名前（**ipv6_pool** など）を入力します。
4. [**Health Monitors**] 設定では、[**Available**] ボックスから、ロードバランスするトラフィックタイプのモニタを選択し、Move ボタン（<<）をクリックして、モニタ名を [**Active**] ボックスに移動します。
5. [**New Members**] 設定では、IPv6 プールメンバを追加します。
   a) [**New Address**] オプションをクリックします。
   b) [**Address**] ボックスに、プール内のノードの IPv6 アドレスを入力します。
   c) [**Service Port**] ボックスに、**80** などのサービス番号を入力するか、[**HTTP**] などのサービス名を選択します。
   d) [**Add**] をクリックします。
   e) プール内のノードごとに、ステップ b、c、および d を繰り返します。
6. [**Finished**] をクリックします。

バーチャルサーバの作成

基本設定の次の作業では、IPv6 ノードのプールを参照するバーチャルサーバを定義します。設定ユーティリティを使用して、バーチャルサーバを作成します。

IPv6 ノード用バーチャルサーバの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**vs_ipv6** など）を入力します。
4. [**Destination**] ボックスで、バーチャルサーバのタイプが [**Host**] になっていることを確認し、[**Address**] ボックスに、バーチャルサーバの IP アドレスを入力します。
5. [**Service Port**] ボックスに、**80** などのサービス番号を入力するか、リストから [**HTTP**] などのサービス名を選択します。
6. 画面の [Configuration] 領域で、[**HTTP Profile**] など、ロードバランスするトラフィックタイプのプロファイル設定を探して、[**http**] などのプロファイル名を選択します。
   これで、選択したプロファイルがバーチャルサーバに割り当てられます。
7. 画面の [Resources] 領域で、[**Default Pool**] 設定を探し、前項で作成したプールの名前を選択します（たとえば、**ipv6_pool**）。
8. [**Finished**] をクリックします。

21

重複したIPアドレスの実装

- 重複したIPアドレスの概要
- ルートドメインの設定

重複した IP アドレスの概要

BIG-IP には、ネットワーク上で重複した IP アドレスを使用する機能があります。この機能は、ルートドメインと呼ばれます。

ルートドメインとは

*ルートドメイン*は、特定のアドレススペースを表すユーザ作成の BIG-IP オブジェクトです。ネットワーク上の独立したルートドメインに個別に配置された複数のノードは、同じ IP アドレスを使用することができます。これにより、たとえば、サービスベンダが複数のプールメンバに同じ IP アドレスを割り当て、各プールメンバが異なる物理サーバを表すことができます。この場合、各プールメンバは、独立したルートドメインに配置されます。ルートドメインを使用する一般的な理由は、それぞれの物理サーバで異なる顧客のトラフィックを処理するためです。

たとえば、2 種類の異なる顧客のトラフィックを処理する場合、2 つの独立したルートドメインを作成できます。同じノードアドレス（たとえば、**10.10.10.1**）を、同じプールまたは別々のプールの両方のルートドメインに配置することができます。また、2 つの対応するプールメンバのそれぞれに別々のモニタを割り当てることができます。

概して、ルートドメインは、主に以下の 2 つの機能を実行します。

- BIG-IP は、あたかも各 IP アドレスに 2 オクテットが別に追加されたように動作します。ただし、ネットワーク上では、4 オクテットの IP アドレスが表示されます。
- それぞれのルートドメインには独自のルーティングテーブルがあり、トラフィックはルートドメインを横切りません。ただし、ルートドメインを横切ように明示的に設定されている場合除きます（デフォルトは拒否）。

ルートドメインの設定には、設定ユーティリティ、**bigpipe** ユーティリティ、または **tmsh** を使用できます。

ルートドメイン ID の指定

作成するルートドメインのそれぞれには、固有な整数の ID が付けられます。重複した IPv4 アドレスを使用するために必要なアドレスフォーマットは、**A.B.C.D%ID** です。ここで、**ID** は、IP アドレスが配置されているルートドメインの ID です。

たとえば、3 つの異なるプールメンバが **10.10.10.1:80** という IP アドレスを使用することができます。ここで、1 つのメンバはルートドメイン **1** に配置され、別のメンバがートドメイン **2**、もう 1 つのメンバがルートドメイン **3** に配置されているとします。この場合、3つのプールメンバは、それぞれ **10.10.10.1%1:80**、**10.10.10.1%2:80**、**10.10.10.1%3:80** として識別されます。

ルートドメインを作成しない場合、作成するすべてのBIG-IPオブジェクトは、デフォルトの単一ルートドメインに配置されます。デフォルトのルートドメインの ID は **0** です。デフォルトのルートドメインのみを使用する場合、IP アドレスに ID **0** を指定する必要はありません。またこの ID は BIG-IP に表示されません。

ルートドメインの設定

標準的なルートドメイン設定を作成するには、ルートドメインごとに以下の BIG-IP オブジェクトを作成します。

- VLAN
- セルフ IP アドレス
- ルートドメインオブジェクト
- プールメンバ
- スタティックルート
- バーチャルサーバ

これらの BIG-IP オブジェクトが IP アドレスを必要とする場合、**%ID** のフォーマットを使用して、関連するルートドメイン ID をアドレスに含める必要があります（ルートドメイン ID については、「*ルートドメイン ID の指定*」（21-1 ページ）を参照してください）。

図 21.1 は、ネットワーク上で重複した IP アドレスを使用することを目的として、2 つの異なるルートドメインを設定する例を示します。この例では、ルートドメイン **1** のオブジェクトと同じ IP アドレスが、ルートドメイン **2** のオブジェクトにも使用されています。これらの重複した IP アドレスの唯一の違いは、固有のルートドメイン ID です。

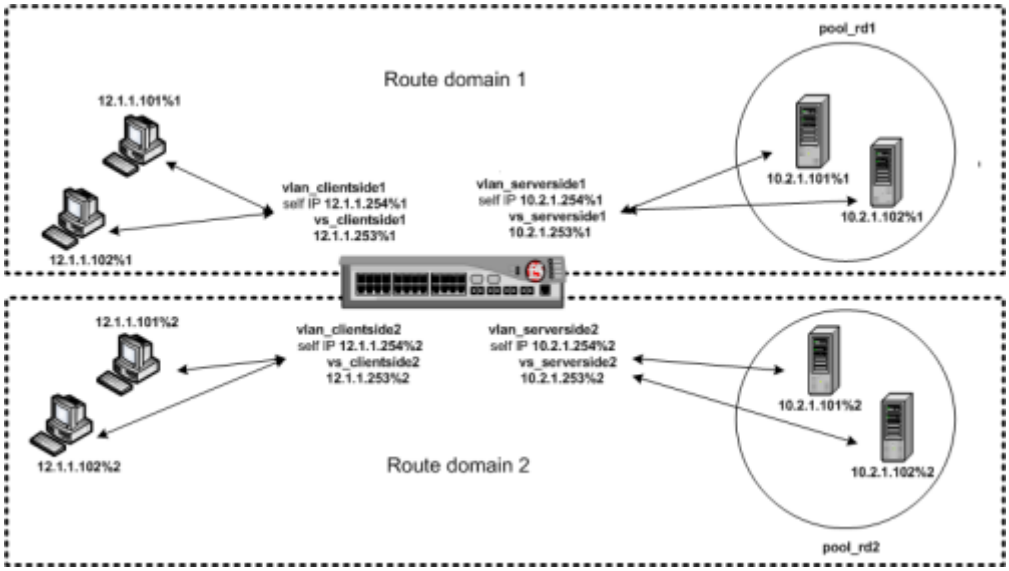

***図 21.1** ルートドメインの設定例*

図 21.1（21-3 ページ）の設定例には、以下のオブジェクトが含まれます。

- **2 つのルートドメイン**
  これらのルートドメインには **1** と **2** の名前が付けられています。
- **ルートドメインごとの 2 つの VLAN**
  ルートドメイン **1** では、これらの VLAN に **vlan_clientside1** と **vlan_serverside1** という名前が付けられています。ルートドメイン **2** では、これらの VLAN に **vlan_clientside2** と **vlan_serverside2** という名前が付けられています。
- **ルートドメインごとの 2 つのセルフ IP アドレス**
  ルートドメイン **1** では、セルフ IP アドレスは **12.1.1.254%1** と **10.2.1.254%1** です。ルートドメイン **2** では、セルフ IP アドレスは **12.1.1.254%2** と **10.2.1.254%2** です。
- **ルートドメインごとの 2 つのクライアントノード**
  ルートドメイン **1** では、クライアント IP アドレスは **12.1.1.101%1** と **12.1.1.102%1** です。ルートドメイン **2** では、クライアント IP アドレスは **12.1.1.101%2** と **12.1.1.102%2** です。
- **ルートドメインごとの 2 つのサーバノード**
  ルートドメイン **1** では、サーバノードの IP アドレスは **10.2.1.101%1** と **10.2.1.102%1** です。ルートドメイン **2** では、サーバノードの IP アドレスは **10.2.1.101%2** と **10.2.1.102%2** です。
- **ルートドメインごとの 2 つの仮想アドレス**
  ルートドメイン **1** では、仮想アドレスは **12.1.1.253%1** と **10.2.1.253%1** です。ルートドメイン **2** では、仮想アドレスは **12.1.1.253%2** と **10.2.1.253%2** です。

◆注

***bigpipe** コマンドや tmsh コマンドの構文については、『**Bigpipe utility Reference Guide**』および『**Traffic Management Shell (tmsh) Reference Guide**』を参照してください。*

ルートドメインに対する VLAN の作成

ルートドメイン作成の最初の手順は、VLAN の作成です。この例では、合計 4 つの VLAN を作成する必要があります。

- ルートドメイン **1** に対応するアプリケーション **A** 用の 2 つの VLAN（**vlan_clientside1** および **vlan_serverside1**）
- ルートドメイン **2** に対応するアプリケーション **B** 用の 2 つの VLAN（**vlan_clientside2** および **vlan_serverside2**）

それぞれの VLAN が作成される際、タグ付きインターフェイス（**1.1** など）が 1 つ付けられます。

ルートドメイン 1 に対する VLAN を作成するには

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**VLANs**] をクリックします。
   既存のすべての VLAN のリストが表示されます。
2. 右上の [**Create**] をクリックします。
   [VLANs] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、VLAN を作成する権限が付与されていません。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
3. [General Properties] 領域で、[**Name**] ボックスに VLAN に一意の名前を入力します。
   この例では、名前は **vlan_clientside1** です。
4. [**Tag**] ボックスに VLAN のタグを入力するか、ボックスを空白のままにします。
   タグを指定しない場合、BIG-IP によって自動的にタグが割り当てられます。
5. [Resources] 領域の [**Interfaces**] 設定で、[**Available**] ボックス内のインターフェイス番号またはトランク名をクリックした後、移動ボタン（[<<] または [>>]）を使用して、インターフェイス番号を [**Tagged**] ボックスに移動します。必要に応じてこの手順を繰り返します。
   タグ付きインターフェイスの詳細については、『***TMOS***™ ***Management Guide for BIG-IP Systems***』を参照してください。
6. 送信元チェックを有効にするには、[Configuration] 領域で [**Source Check**] ボックスをクリックします。
7. [**MTU**] 設定で、デフォルト値を使用するか新しい値を入力します。
8. [**MAC Masquerade**] ボックスに、MAC アドレスを入力します。詳細については、『***TMOS***™ ***Management Guide for BIG-IP Systems***』を参照してください。
9. [**Fail-safe**] 設定で、冗長システムのフェイルオーバーのベースをVLAN関連イベントに置く場合はボックスをオンにします。詳細については、『***TMOS***™ ***Management Guide for BIG-IP Systems***』を参照してください。
10. [**Finished**] をクリックします。
11. この手順を繰り返して、ルートドメイン **1** の 2 番目の VLAN を作成します。このとき、手順 3 では名前 **vlan_serverside1** を割り当てます。

ルートドメイン 2 に対する VLAN を作成するには

設定例の続きとして、上記セクションの手順を使用し、ルートドメイン **2** の VLAN を作成します。このとき、VLAN には名前 **vlan_clientside2** と **vlan_serverside2** を割り当てます。

ルートドメインに対するセルフ IP アドレスの作成

次に、各 VLAN のセルフ IP アドレスを作成します。この例では、ルートドメイン **1** の 2 つの VLAN のそれぞれに 1 つずつ、ルートドメイン **2** の 2 つの VLAN のそれぞれに 1 つずつ、合計 4 つのセルフ IP アドレスを作成します。1 つのルートドメイン内の 2 つのセルフ IP アドレスは固有でなければなりませんが、それぞれのアドレス内のルートドメイン ID が固有である限り、別々のルートドメイン内にある 2 つのセルフ IP アドレスは重複したアドレスでもかまいません。

ルートドメイン 1 の VLAN のセルフ IP アドレスを作成するには

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Self IPs**] をクリックします。
   既存のセルフ IP アドレスのリストが表示されます。
2. 画面の右上の [**Create**] ボタンをクリックします。

   ***注 : [Create]** ボタンをクリックできない場合は、セルフ IP アドレスを作成する権限が付与されていません。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
3. [**IP Address**] ボックスに、VLAN **vlan_clientside1** に割り当てるセルフ IP アドレスを、ルートドメイン ID（**1**）も含めて入力します。
   この例では、**vlan_clientside1** のセルフ IP アドレスは **12.1.1.254%1** です。
4. [**Netmask**] ボックスに、ネットマスクを入力します。
   この例では、ネットマスクは **255.255.255.0** です。
5. [**VLAN**] 設定で、セルフ IP アドレスに割り当てる VLAN の名前を選択します。
   この例では、名前は **vlan_clientside1** です。
6. [**Port Lockdown**] 設定で、[**Allow Default**] を選択します。
7. セルフ IP アドレスをフローティング IP アドレスとして設定するには、[**Floating IP**] ボックスをオンにします。
8. このセルフ IP アドレスの設定を終了してほかのセルフ IP アドレスを作成するには、[**Repeat**] をクリックし、すべてのセルフ IP アドレスが作成されるまで、前のステップをすべて実行します。
9. [**Finished**] をクリックします。
10. この手順を繰り返して、ルートドメイン **1** のもう 1 つの VLAN のセルフ IP アドレスを作成します。
    この例では、セルフ IP アドレスは **10.2.1.254%1**、VLAN は **vlan_serverside1** です。

ルートドメイン2のVLANのセルフIPアドレスを作成するには

設定例の続きとして、上記セクションの手順を使用し、ルートドメイン **2** の VLAN のセルフ IP アドレスを作成します。ルートドメイン **2**VLAN のセルフ IP アドレスは、ルート ID が異なる以外はルートドメイン **1** のアドレスと同じです。この例では、ルートドメイン **2** のセルフ IP アドレスは、**12.1.1.254%2** と **10.2.1.254%2** であり、これらのアドレスを VLAN **vlan_clientside2** および **vlan_serverside2** に割り当てます。

ルートドメインオブジェクトの作成

次に、ルートドメインオブジェクトを作成します。この例では、2 つのルートドメインオブジェクトを作成し、2 つの既存の VLAN を各ルートドメインに割り当てます。

ルートドメイン I に対するルートドメインオブジェクトを作成するには

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Route Domains**] をクリックします。
   既存のルートドメインのリストが表示されます。
2. 画面の右上の [**Create**] ボタンをクリックします。

   注 :[Create] *ボタンをクリックできない場合は、セルフ IP アドレスを作成する権限が付与されていません。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
3. [**ID**] ボックスに、整数のルートドメイン ID を入力します。
   この例では、値は **1** です。
4. [**Description**] ボックスに、ルートドメインの説明テキストを入力します。
5. [**Parent ID**] ボックスから、[**None**] を選択します。
6. [VLAN] 設定では、[**Available**] ボックスで VLAN 名 **vlan_clientside1** をクリックし、移動ボタン（[<<] または [>>]）を使用して名前を [**Members**] ボックスに移動します。VLAN 名 **vlan_serverside1** について、この手順を繰り返します。
7. [**Finished**] をクリックします。

ルートドメイン 2 に対するルートドメインオブジェクトを作成するには

設定例の続きとして、上記セクションの手順を使用し、ルートドメイン **2** を作成します。このとき、ルートドメインには VLAN**vlan_clientside2** と **vlan_serverside2** を割り当てます。

ルートドメインに対するプールメンバの作成

次に、各ルートドメインに対するプールとプールメンバを作成する必要があります。設定例の続きとして、各プールのプールメンバを作成し、プールメンバのアドレスにルートドメイン ID を指定します。

この例では、各ルートドメインは同じプールメンバのセットを使用します。各ルートドメイン内のルートドメイン ID のみ異なります。したがって、ルートドメイン **1** と **2** のそれぞれには、同じプールメンバ **10.2.1.101:80** および **10.2.1.102:80** があります。

ルートドメイン 1 に対するプールメンバを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   既存のプールのリストが表示されます。
2. 画面の右上の [**Create**] ボタンをクリックします。

   ***注：** [Create] ボタンをクリックできない場合は、プールを作成する権限が付与されていません。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
3. [**Name**] ボックスに、プールの名前（**pool_rd1** など）を入力します。
4. [**Health Monitors**] 設定では、[**Available**] ボックスでモニタを選択し、Move ボタン（[<<] または [>>]）を使用して、そのモニタを [**Active**] ボックスに移動します。
5. [**New Members**] 設定で、以下の作業を行います。
   a) [**Address**] ボックスに、ルートドメイン ID を含めたプールメンバアドレスを入力します。この例では、アドレスは **10.2.1.101%1** です。
   b) [**Service Port**] ボックスでは、サービス名を入力するか、リストからサービスを選択します。
   c) [**Add**] をクリックします。
   d) 2 番目のプールメンバに対して、手順 a、b、c を繰り返します。この例では、アドレス **10.2.1.102%1** を使用します。
6. [**Finished**] をクリックします。

ルートドメイン 2 に対するプールメンバを作成するには

設定例の続きとして、上記セクションの手順を使用し、ルートドメイン **2** のプールメンバを作成します。この例では、**pool_rd2** という名前のプールを作成し、IP アドレス **10.2.1.101%2** および **10.2.1.102%2** をプールメンバに割り当てます。これらは、ルートドメイン ID を除き、**pool_rd1** のメンバに対して指定した IP アドレスと同じです。

スタティックルートの作成

次に、各ルートドメインに適用するスタティックルートを作成する必要があります。この例では、ルートドメインごとに、クライアント側とサーバ側の両方の宛先にルートが適用されます。

ルートドメイン 1 に対するスタティックルートを作成するには

1. ナビゲーションペインの [Main] タブで、[**Network**] を展開して [**Routes**] をクリックします。
   [Routes] 画面が開きます。
2. 画面の右上で [**Add**] をクリックします。

   注：[Add] *ボタンをクリックできない場合は、スタティックルートを作成する権限が付与されていません。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
3. [**Type**] リストから、[**CRLDP**] を選択します。
4. [**Destination**] ボックスに、ルートドメイン ID を含めた宛先 IP アドレスを入力します。
   たとえば、宛先としてプールメンバのノードアドレスを指定できます（**pool_rd1** の **10.2.1.101%1** など）。
5. [**Netmask**] ボックスに、[**Destination**] ボックスに入力した IP アドレスのネットマスクを入力します。
6. [**Resource**] プロパティで、以下のいずれかを選択します。

   a) **Use Gateway**
   ボックスに、ルートドメイン **1** 内の VLAN のセルフ IP アドレスを入力します。たとえば、**vlan_serverside1** のセルフ IP アドレスの場合なら、**10.2.1.254%1** などと入力します。

   b) **Use VLAN**
   ボックスに、ルートドメイン **1** 内の VLAN の名前（**vlan_serverside1** など）を入力します。
7. [**Finished**] をクリックします。
8. 設定例の続きとして、上記の手順を繰り返し、ルートドメイン **1** に対する他のスタティックルートを作成します。

   a) **pool_rd1**内の他のサーバ側ノード へのルート（**10.2.1.102%1**）。この場合、ゲートウェイアドレスおよび VLAN 名は、手順 1 ～ 7 で作成したルートと同じです（それぞれ **10.2.1.254%1** および **vlan_serverside1**）。

   b) ルートドメイン **1** 内のクライアント側ノードへのルート。この例の場合、宛先アドレスは **12.1.1.101%1**、ゲートウェイアドレスは **12.1.1.254%1**、VLAN 名は **vlan_clientside1** です。

   c) ルートドメイン**1**内の他のクライアント 側ノード へのルート 。この例の場合、宛先アドレスは **12.1.1.102%1**、ゲートウェイアドレスと VLAN 名は上記の手順と同じ（それぞれ **12.1.1.254%1** および **vlan_clientside1**）です。

ルートドメイン 2 に対するスタティックルートを作成するには

設定例の続きとして、上記セクションの手順を使用し、ルートドメイン **2** のスタティックルートを作成します。この場合、以下のルートを作成します。

- **pool_rd2** 内の 2 つのサーバ側ノード（ノード **10.2.1.101%2** と **10.2.1.102%2**）のそれぞれに対応する 2 つのルート）。ゲートウェイアドレス **10.2.1.254%2** または VLAN 名 **vlan_serverside2** のいずれかを指定します。
- 2つのクライアント側ノード（ノード **12.1.1.101%2** と **12.1.1.102%2**）のそれぞれに対応する 2 つのルート。ゲートウェイアドレスと VLAN 名は、それぞれ **12.1.1.254%2** と **vlan_clientside2** です。

ルートドメインに対するバーチャルサーバの作成

最後に、それぞれのルートドメインに対するバーチャルサーバを作成し、各バーチャルサーバにプールを割り当てる必要があります。この例では、**pool_rd1** 内の 2 つのノードが使用する 2 つのプールメンバアドレスは、**pool_rd2** のノードのアドレスと同じです。ただし、プールメンバアドレスに指定されたルートドメイン ID はルートドメインごとに異なります。

ルートドメイン 1 に対するバーチャルサーバを作成するには

1. [Main] タブで [**Local Traffic**] を展開し、[**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面の右上の [**Create**] ボタンをクリックします。
   [New Virtual Server] 画面が開きます。

   注 :[Create] *ボタンをクリックできない場合は、現在のユーザロールではバーチャルサーバを作成する権限が与えられていないことを示します。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
3. [**User Name**] ボックスに、ルートドメイン 1 内のバーチャルサーバの名前を入力します
   （たとえば、**vs_serverside_rd1** など）。
4. [**Destination**] ボックスで次の作業を行います。

   a) [**Host**] ボタンが選択されていることを確認します。

   b) [**Address**] ボックスにバーチャルサーバの IP アドレスを入力します（たとえば、**10.2.1.253%1** など）。
5. [**Service Port**] ボックスにサービス番号（**80** など）を入力するか、リストからサービス名（**HTTP** など）を選択します。
6. [**State**] が [**Enabled**] に設定されていることを確認します。

7. [**Configuration**] リストから、[**Advanced**] を選択し、以下の作業を実行します。

   a) [**Type**] リストから [**Performance (Layer 4)**] を選択します。このバーチャルサーバタイプの詳細については、『***Configuration Guide for BIG-IP Local Traffic Management***』を参照してください。

   b) [**Default Pool**] の設定以外は、デフォルト値をそのまま使用します。

8. [**Default Pool**] リストから、ルートドメイン **1** のプールの名前を選択します。
   この例では、プール名は **pool_rd1** です。

9. [**Finished**] をクリックします。

10. この手順を繰り返して、ルートドメイン **1** のクライアント側バーチャルサーバを作成します。
    この例では、バーチャルサーバ名は **vs_clientside_rd1**、バーチャルサーバアドレスは **12.1.1.253%1** です。デフォルトのプール名を選択する場合、手順 8 は省略できます。

ルートドメイン 2 に対するバーチャルサーバを作成するには

設定例の続きとして、上記セクションの手順を使用し、ルートドメイン **2** のバーチャルサーバを作成します。

- IP アドレスが **10.2.1.253%2** のバーチャルサーバを作成し、**vs_serverside_rd2** などの名前を付けます。
- IP アドレスが **12.1.1.253%2** のバーチャルサーバを作成し、**vs_clientside_rd2** などの名前を付けます。デフォルトのプール名を選択する場合、手順 8 は省略できます。

22

サービス拒否攻撃やその他の攻撃の緩和

- 基本的なサービス拒否攻撃に対するセキュリティ の概要
- アダプティブコネクションリーパの設定
- 単純な DoS 攻撃の防御設定
- iRule を使用した攻撃のフィルタ除去
- BIG-IP での、一般的なさまざまな攻撃への対処方法

基本的なサービス拒否攻撃に対するセキュリティの概要

BIG-IP には、ネットワークのセキュリティ対策を目的とした設定を作成する場合に役に立つ、複数の機能や設定が用意されています。BIG-IP は、システムリソースを消費して受信者へのサービスを拒否させようとするサービス拒否（DoS）攻撃の影響を軽減するという点で特にその機能を発揮します。

次に挙げる BIG-IP の機能は、さまざまな DoS 攻撃を阻止する上で役立ちます。

- **堅固な専用カーネル**
  BIG-IP カーネルには、同時接続を制限したり、未承認の SYN や ACK パケットが含まれる接続を一定時間の経過後に切断することにより、SYN フラッド攻撃からシステムを防御するメカニズムが組み込まれています（***SYN*** **や*****ACK*** パケットは、TCP3 ウェイハンドシェイクの一部として送信されるパケットです）。
- **高パフォーマンス**
  BIG-IP は、1 秒あたり数万ものレイヤ 4（L4）接続を処理できます。十分なサーバリソースおよび帯域幅が利用可能であれば、BIG-IP 自体またはサイトのどちらかに影響を及ぼすまでに至るには、かなり決定的な攻撃が必要になります。
- **大容量メモリ**
  SYN フラッド攻撃またはサービス拒否（DoS）攻撃では、利用可能なすべてのメモリが消費されることがあります。BIG-IP は大容量のメモリをサポートしており、DoS 攻撃の阻止に役立ちます。

この章では、DoS 攻撃の緩和に役立つ、いくつかの設定について説明します。次の設定について説明します。

- BIG-IP による攻撃対応を目的とするアダプティブコネクションリーパの設定方法（次項）
- サービス拒否攻撃からの防御を目的とする基本設定（22-4 ページ）
- 既知の特定攻撃のフィルタ除去に使用する iRule™ の構文例（22-7 ページ）

これらの作業の詳細については、設定ユーティリティの [Help] タブまたは『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

アダプティブコネクションリーパの設定

BIG-IP には、アダプティブコネクションリーパ実現する 2 つのグローバル設定が用意されています。***コネクションリーパ*** は、積極的なリープの開始をトリガするだけのメモリが、接続負荷によって使用されると、BIG-IP から接続を排除するという状況です。サービス拒否攻撃から防御するために、最低点のしきい値と最高点のしきい値を指定できます。

- ***最低点*** のしきい値は、アダプティブコネクションリーパがより積極的になる時点を決定します。
- ***最高点*** のしきい値は、BIG-IP を介する未確立の接続が許可されないようになる時点を決定します。この変数の値は、メモリ利用率を表します。

メモリ利用率が最高点に達すると、利用可能なメモリが最低点のしきい値まで緩和されるまで、接続は拒否されます。

◆ 警告

*アダプティブコネクションリーパの設定は、SSL 接続には適用されません。ただし、アイドル状態の SSL 接続をリープする TCP や UDP 接続タイムアウトは設定できます。詳細については、「**TCP および UDP 接続タイマの設定**」（22-4 ページ）を参照してください。*

設定ユーティリティを使用したアダプティブコネクションリーパの設定方法

1. ナビゲーションペインの [Main] タブで、[**System**] を展開して [**Configuration**] をクリックします。
   [General] 画面が開きます。
2. [Local Traffic] メニューから、[General] を選択します。
   [System] 画面が開きます。
3. [Properties] テーブルで、次の値を設定します。
   - [**Reaper High-water Mark**] プロパティを **95** に設定します。
   - [**Reaper Low-water Mark**] プロパティを **85** に設定します。
4. [**Update**] をクリックします。

◆ ヒント

これらの値は、ほとんどの BIG-IP の配置に対して最適なソリューションを表しているため、通常変更する必要はありません。

◆ 重要

*両方のアダプティブコネクションリーパ値を **100** に設定すると、この機能は無効になります。*

アダプティブコネクションリーパの活動の記録

BIG-IP でのログレベルをより高い機密性レベルに設定して、アダプティブコネクションリーパの活動を記録できます。

このログレベルを設定すると、システムは、レート制限されたメッセージ（最高 10 秒ごとに 1 度）を記録し、アダプティブコネクションリーパの開始または終了を知らせます。このログメッセージには、**警告**の優先度が与えられています。ログレベルの詳細については、**db** のマニュアルページを参照してください。

◆ 重要

*アダプティブコネクションリーパの最高点限度に達すると、LCD にメッセージ **Blocking DoS Attack** が表示されます。*

コマンド行からのアダプティブコネクションリーパのログレベルの設定方法

1. BIG-IP でコンソールを開きます。
2. 次のコマンドを入力して、アダプティブコネクションリーパのログレベルを表示します。

   ```
   bp db Log.DosProtect.Level list
   ```

   出力は次のようになります。

   ```
   db Log.DosProtect.Level "Warning"
   ```

3. アダプティブコネクションリーパのログレベルを選択します。次のレベルでは、**Reaper High Water Mark** を超過すると、LCD にメッセージ **Blocking DoS Attack** が表示されます。

   - Emergency（緊急）
   - Alert（アラート）
   - Critical（重要）
   - Error（エラー）
   - Warning（警告）

   次のレベルは、LCD にメッセージ **Blocking DoS Attack** は表示されません。

   - Notice（注意）
   - Informational（通知）

4. 次のコマンドを入力して、アダプティブコネクションリーパのログレベルを設定します。ただし、**<log level>** はログレベルになります。

   ```
   bp db Log.DosProtect.Level "<log level>"
   ```

単純な DoS 攻撃の防御設定

DoS 攻撃の防御は、サービス拒否攻撃の影響を軽減するために利用できる単純な設定です。

この設定は、次の 4 つの作業から構成されます。

- グローバルTCPおよびUDP接続のリープタイムを60秒に設定する。
- IP レートクラスを 20Mbps に、未処理キューの最大サイズを 2Mbps に設定する。
- 主要バーチャルサーバでの接続制限を、RAM（KB）*0.8 に近似した容量に設定する。

TCP および UDP 接続タイマの設定

TCP プロファイルと UDP プロファイルのプロファイル設定で、TCP およびUDPタイマを設定できます。バーチャルサーバで使用するサービスに合わせて、これらのタイマを設定します。たとえば、HTTP 接続に対して **60**、SSL 接続に対して **60** を設定します。

TCP 接続のリーパタイムの設定方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. [Protocol] メニューから、TCP を選択します。
   [TCP Profile List] 画面が開きます。
3. 設定するプロファイルの名前をクリックします。
   プロファイルのプロパティ画面が開きます。
4. [**Idle Timeout**] を **60** に設定します。
5. [**Update**] をクリックします。

UDP 接続のリーパタイムの設定方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. [Protocol] メニューから、UDP を選択します。
   [UDP Profile List] 画面が開きます。
3. 設定するプロファイルの名前をクリックします。
   プロファイルのプロパティ画面が開きます。
4. [**Idle Timeout**] を **60** に設定します。
5. [**Update**] をクリックします。

IP レートクラスの作成とバーチャルサーバへの適用

DoS 攻撃に対する単純な設定の次の作業では、レートクラスを作成します。まずレートクラスを作成し、そのレートクラスをバーチャルサーバへ適用します。

◆ 重要

レートクラスモジュールには、ライセンスキーが必要になります。この機能がなく、ライセンスキーを購入する場合は、F5 ネットワークスにお問い合わせください。

レートクラスの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Rate Shaping**] をクリックします。
   [Rate Shaping] 画面が表示されます。
2. [**Create**] ボタンをクリックして、新しいレートクラスを作成します。
   [New Rate Class] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではレートクラスを作成する権限が与えられていないことを示します。*
3. 次のクラスプロパティを設定します。
   - [**Class Name**] ボックスに、このクラスに使用する名前を入力します。
   - [**Base Rate**] ボックスに **2000000**（2Mbps）と入力します。
   - [**Ceiling Rate**] ボックスに **20000000**（20Mbps）と入力します。
   - [**Burst Size**] ボックスに、**500** と入力するか、リストから [**Megabytes**] を選択します。
   - [**Direction**] リストから、[**Any**] を選択します。
   - [**Queue Discipline**] リストから、[**Stochastic Fair Queue**] を選択します。
4. [**Finished**] をクリックします。

レートクラスを作成したら、設定内のバーチャルサーバにそのレートクラスを適用できます。

レートクラスのバーチャルサーバへの適用方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers List] 画面が開きます。
2. [Virtual Servers List] 画面で、修正するバーチャルサーバをクリックします。
3. [**Rate Class**] リストから、作成したレートクラスを選択します。
4. [**Update**] をクリックします。

主要バーチャルサーバでの接続制限の設定

この項では、主要バーチャルサーバでの接続制限の設定方法について説明します。接続制限は、バーチャルサーバで許可される最大の同時接続数を決定します。ここでは、主要バーチャルサーバは、サイトへの最大のトラフィックを受信するバーチャルサーバになります。

主要バーチャルサーバでの接続制限の算出方法

接続制限を設定する前に、次の公式を使用して、主要バーチャルサーバで接続制限に設定する数値を算出します。

接続制限 = RAM（KB）*0.8 に近似した容量

たとえば、RAM が 256MB の場合、計算は次のようになります。

256,000 * 0.8 = 20480

この例では、接続制限を **20480** に設定します。

主要バーチャルサーバでの接続制限を設定するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers List] 画面が開きます。
2. [Virtual Servers List] 画面で、修正するバーチャルサーバをクリックします。
3. [**Connection Limit**] ボックスに、接続制限として計算した数値を入力します。
4. [**Update**] ボタンをクリックします。

iRule を使用した攻撃のフィルタ除去

BIG-IP 上でルールを作成して、不正な DoS 攻撃をフィルタ除去できます。特定の攻撃を識別したら、パケットを不正と特定する要素が含まれるパケットを廃棄する iRule を作成できます。

Code Red 攻撃のフィルタ除去

BIG-IP は、HTTP 要求をダミープールに送信する iRule を使用して、Code Red 攻撃をフィルタ除去できます。たとえば、図 22.1 は、Code Red 攻撃を廃棄する iRule を示しています。

```
when HTTP_REQUEST {
  if {string tolower [HTTP::uri] contains "default.ida" } {
     discard
  } else {
     pool RealServerPool
 }
}
```

***図 22.1** Code Red 攻撃に対するフィルタ除去のサンプル iRule*

Nimda 攻撃のフィルタ除去

Nimda ワームは、Microsoft® Windows® オペレーティングシステムを基盤とするシステムやアプリケーションを攻撃の対象としています。Nimda の場合、図 22.2 に示すように iRule を作成できます。

```
when HTTP_REQUEST {
  set uri [string tolower [HTTP::uri]]
  if { ($uri contains "cmd.exe") or ($uri contains
"root.exe") or ($uri contains "admin.dll") } {
     discard
  } else {
    pool ServerPool
 }
}
```

***図 22.2** Nimda ワームを廃棄する iRule の構文サンプル*

BIG-IP での、一般的なさまざまな攻撃への対処方法

サービスデバイスやネットワークデバイスを停止させてサービス拒否を引き起こすような一般的な攻撃に対して、BIG-IP がどのように対処しているかを説明します。

以降のページでは、最も一般的な攻撃を取り上げ、それぞれの攻撃に対して BIG-IP の機能がどのように対応しているかを示します。

◆警告

アイドルセッションリープタイムアウトを低く設定するときは、必ず注意してください。アプリケーションが時間内に応答できない場合に、有効な接続がリープされてしまうことがあります。

SYN フラッド

SYN フラッド は、システムリソースの消費を目的とするシステム攻撃です。対象のシステムに対して SYN フラッドを開始した攻撃者は、不正な IP アドレスを含んだ複数の SYN セグメントを送信し、TCP 接続の確立に使用されるリソースをすべて占有しようとします。***SYN*** の用語は、TCP/IP 接続の確立時に発生する接続状態のタイプを示します。

より具体的に説明すると、SYN フラッドは SYN キューを一杯にするように意図されています。***SYN キュー***とは、標準的な 3 ウェイハンドシェイクの一部として、SYN-RECEIVED 状態で接続テーブルに保存された一連の接続のことです。SYN キューは、指定した最大数の、SYN-RECEIVED 状態の接続を保持します。

SYN-RECEIVED 状態の接続は、ハーフオープン状態で、クライアントからの確認応答待ちとみなされます。SYN フラッドによって、SYN-RECEIVED 状態の接続が許容最大数に達すると、SYN キューは一杯になったとみなされ、その結果、対象のシステムは他の正当な接続を確立できなくなります。したがって、SYN キューが一杯になると、存在しないまたは到達できない IP アドレスに対して一部が開いた TCP 接続が生じます。このような場合、接続がそのタイムアウトに達し、サーバは他の要求への対応を続行できなくなります。

SYN フラッドの緩和

BIG-IP には、SYN フラッドの緩和を目的とした機能が用意されています。この機能は、***SYN Check*** と呼ばれ、フローに関する情報を要求側のクライアントへ Cookie 形式で送信します。このため、通常は開始されたセッション用に接続テーブルに保存される SYN-RECEIVED 状態を、システムで保持する必要がなくなります。接続のたびに SYN-RECEIVED 状態が保持されないので、SYN キューは消費されず、通常の TCP 通信を継続できます。

SYN Check 機能は、BIG-IP の既存のアダプティブコネクションリーパ機能を補完します。アダプティブコネクションリーパが確立後の接続フラッドを処理するのに対して、SYN Check は、接続フラッドを完全に防止します。つまり、アダプティブコネクションリーパは、接続をフラッシュするために長時間にわたって機能する必要がありますが、SYN Check 機能は、SYN キューが一杯になることを防ぐため、対象のシステムは継続して TCP 接続を確立することができます。

システム上で接続の何らかのしきい値に達したときに、SYN Check 機能を有効にするように BIG-IP を設定できます。

BIG-IP でのしきい値の設定方法

1. ナビゲーションペインの [Main] メニューで、[**System**] を展開して [**Configuration**] をクリックします。
   [General Properties] 画面が開きます。
2. [Local Traffic] メニューから、[General] を選択します。
   [General] 画面が開きます。
3. [**SYN Check™ Activation Threshold**] ボックスに、しきい値に定義する接続数を入力します。
4. [**Update**] をクリックします。

ICMP フラッド（スマーフ）

ICMP フラッドは、「スマーフ」攻撃とも呼ばれ、基本的にはリモートネットワークから 1 つのホストへ ICMP エコーリプライを送信させる攻撃です。この攻撃では、攻撃者からの単一のパケットが、保護されていないネットワークのブロードキャストアドレスに送られます。通常、この結果、攻撃対象のシステムに送信されたパケットが、そのネットワーク内のすべてのコンピュータから返されます。

BIG-IP では、1 秒あたりに応答する ICMP 要求数を限定し、それ以外は破棄するため、このような攻撃に対して堅固です。

BIG-IP 内部のネットワークでは、BIG-IP は、ダイレクトされたサブネットブロードキャストを無視し、スマーフ攻撃者が攻撃の開始に使用するブロードキャスト ICMP エコーには応答しません。

このタイプの攻撃に対して、BIG-IP のシステム設定に変更を加える必要は一切ありません。

UDP フラッド

UDP フラッド攻撃は、最も一般的な分散サービス拒否（DDoS）攻撃です。この場合、複数のリモートシステムから、大量の UDP パケットが対象のシステムに送信されます。

BIG-IP では、SYN フラッドへの対応処理方法と同様に、これらの攻撃に対処します。ポートがリッスンしていない場合は、BIG-IP がパケットを破棄します。ポートがリッスンしている場合は、リーパが不正な接続を切断します。

UDP アイドルセッションタイムアウトを 5 から 10 秒の間に設定すると、これらの接続はすばやくリープされ、ユーザは接続速度の低下の影響を受けることはありません。ただし UDP の場合は、5 から 10 秒の設定では非常に多くのオープンな接続が残る可能性があり、状況によっては、2 から 5 秒の間に設定する必要があります。

UDP フラグメント

UDP フラグメント攻撃は、基本的にフラグメント化パケットとして送信された大量の UDP データをシステムで再構築させます。この攻撃は、システムがダウンするまで、システムリソースを消費させることが目的です。

BIG-IP では、これらのパケットを再構築しません。パケットはオープンな UDP サービス向けである場合に、サーバに送信されます。これらのパケットが、正常に接続を開始する初期パケットといっしょに送信された場合、この接続は、バックエンドサーバに送信されます。初期パケットがストリームの最初のパケットでない場合は、ストリーム全体が破棄されます。

このタイプの攻撃に対して、BIG-IP のシステム設定に変更を加える必要は一切ありません。

Ping of Death

Ping of Death 攻撃は、65535 バイトを超える ICMP エコーパケットを使用した攻撃です。これは最大許容サイズの ICMP パケットであるため、システムは、このパケットを再構築しようとするとクラッシュします。

BIG-IP は、このタイプの攻撃に対して堅固です。ただし、この攻撃が **Any IP** 機能を有効にしたバーチャルサーバに向けられている場合は、これらのパケットはサーバに送信されます。最新の更新パッチをサーバに適用しておくことが重要です。

このタイプの攻撃に対して、BIG-IP のシステム設定に変更を加える必要は一切ありません。

Land 攻撃

Land 攻撃は、SYN パケットの送信元のアドレスとポートを攻撃対象のサーバのアドレスとポートと同じに細工します。

BIG-IP は、この攻撃に対して堅固です。BIG-IP の接続テーブルは既存の接続と一致しているため、この種のなりすましはサーバに送信されません。BIG-IP への接続はチェックされ、このようなすましがあると破棄されます。

このタイプの攻撃に対して、BIG-IP のシステム設定に変更を加える必要は一切ありません。

Teardrop

Teardrop 攻撃は、インターネットまたはネットワークに接続したコンピュータへ、IP フラグメントを送信するプログラムによって実行されます。Teardrop 攻撃は、いくつかの一般的なオペレーティングシステムに存在する重複した IP フラグメント問題を利用します。この問題のために、TCP/IP フラグメンテーションの再構築コードが、重複した IP フラグメントを間違って処理するという事態が起こります。

BIG-IP は、フレームの配列が正しいかどうかを調べ、不適切な配列のフラグメントを破棄して、これらの攻撃に対処します。

このタイプの攻撃に対して、BIG-IP のシステム設定に変更を加える必要は一切ありません。

データ攻撃

BIG-IP はまた、BIG-IP の内側のサーバに対するデータ攻撃からの保護機能も備えています。BIG-IP はポート拒否デバイスとして機能し、単純に攻撃がサーバにまで及ばないようにして、一般多数の不正利用を防止します。

一般的な 2 つのデータ攻撃について、攻撃を防止する iRule の例は、「*iRule を使用した攻撃のフィルタ除去*」（22-7 ページ）を参照してください。

WinNuke

WinNuke 攻撃は、特定の一般的なオペレーティングシステムの、NetBIOS ポートへの送信データの処理方法を悪用します。NetBIOS ポートは **135**、**136**、**137**、および **138** であり、TCP または UDP を使用します。BIG-IP は、デフォルトでこれらのポートを拒否します。

この攻撃に対するパッチがサーバに適用されているかどうか確信がない場合は、BIG-IP でこれらのポートを開かないでください。

Sub 7

Sub 7 攻撃はトロイの木馬で、一般的なオペレーティングシステムで実行するように作られています。このトロイの木馬は、リモートでシステムを制御できます。

また、デフォルトで、ポート **27374** でリッスンします。BIG-IP は、このポートに外部からの接続を許可しないため、攻撃を受けたサーバをリモートで制御することはできません。

これらのポートで実行中のアプリケーションを明確に把握できない限り、上位ポート（**1024** よりも上のポート）は開かないでください。

Back Orifice

Back Orifice 攻撃はトロイの木馬で、一般的なオペレーティングシステムで実行するように作られています。このトロイの木馬は、リモートでシステムを制御できます。

また、デフォルトで、UDP ポート **31337** でリッスンします。BIG-IP は、このポートに外部からの接続を許可しないため、攻撃を受けたサーバをリモートで制御することはできません。これらのポートで実行中のプログラムを明確に把握できない限り、上位ポート（**1024** よりも上のポート）は開かないでください。

23

管理ドメインの設定

- 管理ドメインの概要
- パーティションの作成
- パーティションに対するユーザアクセスの設定
- パーティション内のオブジェクトの表示、管理、作成

管理ドメインの概要

BIG-IP® には、管理ドメインと呼ばれる強力な承認機能があります。*管理ドメイン*機能を使用することにより、BIG-IP のシステムリソースへの適切なタイプのアクセスが適切な量だけ BIG-IP から管理ユーザに付与されることを保証できます。その結果、組織のニーズに正確に合うように、各種リソースへのユーザアクセスを調整することができます。

管理ドメイン機能は、以下の重要コンポーネントで構成されています。

- **パーティション**
  *パーティション*は、BIG-IP システムオブジェクトのコンテナを表します。パーティションを使用して、ユーザアクセスを特定のオブジェクトに制限することができます。パーティションの詳細については、『***TMOS™ Management Guide for BIG-IP Systems***』を参照してください。
- **ユーザアカウント**
  *ユーザアカウント*は、BIG-IP への管理アクセスを付与します。ユーザアカウントに設定したプロパティにより、BIG-IP システムリソースを管理するためのユーザ権限が決定されます。ユーザアカウントの詳細については、『***TMOS™ Management Guide for BIG-IP Systems***』を参照してください。
- **ユーザロール**
  ユーザアカウントに設定するプロパティの 1 つのがユーザロールです。*ユーザロール*により、ユーザの権限が決まります。すなわち、ユーザがアクセスできるオブジェクトと、ユーザが実行できるタスクが決定されます。ユーザアカウントに割り当てることができるユーザロールは、**Administrator**、**Resource Administrator**、**User Manager**、**Manager**、**Application Editor**、**Application Security Policy Editor**、**Operator**、**Guest** のいずれかです。また、特定のユーザアカウントがシステムリソースへのアクセス権限を持たないように指定することもできます。これらのユーザロールについては、『***TMOS™ Management Guide for BIG-IP Systems***』を参照してください。
- **BIG-IP システムオブジェクト**
  BIG-IP システム*オブジェクト*は、BIG-IP 上で管理可能なエンティティです。パーティション内に配置可能なオブジェクトの例としては、プール、バーチャルサーバ、プロファイルなどがあります。オブジェクトがパーティション内にある場合には、これらのオブジェクトに対する管理ユーザアクセスのタイプと量を制御できます。ユーザアカウントと同様に、ほとんどのローカルトラフィックオブジェクトもパーティション内に配置できます。ローカルトラフィックオブジェクトについては、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。

これらのコンポーネントをすべて組み合わせることにより、多くの BIG-IP システムリソースに対する管理アクセスをきめ細かく調整することができます。この章では、BIG-IP の管理ドメイン機能の設定手順について説明します。

パーティションの作成

BIG-IP を最初にインストールしたときには、**Common** と呼ばれるデフォルトのパーティションが存在します。***Common*** パーティションには、**admin** ユーザアカウント、デフォルトのプロファイル、事前設定済みのヘルスモニタおよびパフォーマンスモニタなど、インストール時にシステムが自動的に作成するオブジェクトが含まれます。

BIG-IP システムオブジェクトのタイプによっては、パーティション内に配置されるものや、そうでないものがあります。通常、ほとんどのローカルトラフィックオブジェクトは、パーティション内にあります。セルフ IP アドレス、VLAN、インターフェイスなどのネットワークオブジェクトは、パーティション内に配置できません。

ほとんどの BIG-IP システムユーザアカウントは、そのユーザロールに関わらず、最低限、**Common** パーティション内にオブジェクトに対する Read アクセス権限を持ちます。**Administrator** ロールおよび **Resource Administrator** ロールが割り当てられたユーザアカウントは、**Common** パーティション内のオブジェクトの表示ができるだけでなく、そのパーティション内でオブジェクトの作成、変更、削除もできます。

Common パーティションの管理は、BIG-IP システムオブジェクトへのユーザアクセスを制御するための開始点として有効ですが、別のパーティションを追加作成することにより、管理ユーザのアクセス制御が格段にきめ細かく行えるようになります。

特定のパーティション内のオブジェクトを管理する権限をユーザに与えるための最初の手順は、パーティションの作成です。パーティションの作成が終了したら、新しいパーティション内のオブジェクトを管理するユーザを選択します。最後に、そのユーザのアカウントのプロパティを変更し、該当するユーザロールと、そのユーザに管理を許可するパーティションの両方を割り当てます。パーティション管理の権限をユーザに付与すると、そのユーザは、そのパーティション内のオブジェクトを特定の方法（たとえば、HTTP バーチャルサーバやプロファイルの作成など）で管理できるようになります。

◆ 重要

*パーティションを作成するには、ユーザアカウントに **Administrator** ユーザロールまたは **Resource Administrator** ユーザロールを割り当てる必要があります。**admin** アカウントに対しては、BIG-IP が自動的に **Administrator** ロールを割り当てます。*

パーティションを作成するには

1. ナビゲーションペインの [Main] タブで、[**System**] を展開して [**Users**] をクリックします。
   [Users] 画面が開きます。
2. メニューバーの [**Partitions List**] をクリックします。
   ここには、現在の権限で表示可能なパーティションの一覧が表示されています。
3. 画面の右上で [**Create**] をクリックします。

4. [**Name**] ボックスに、パーティションの固有な名前（**partition_App1** など）を入力します。
5. [**Description**] ボックスに、パーティションの説明を入力します。たとえば、「**このパーティションには、App1 アプリケーションのトラフィックを管理するためのオブジェクトが含まれます。**」などとします。
6. [**Create**] をクリックします。

パーティションに対するユーザアクセスの設定

パーティション作成の次のステップは、ユーザロールをユーザアカウントに割り当て、作成した新しいパーティションを管理する権限をそのユーザに与えます。ユーザに与えられる権限のレベルは、ユーザアカウントに割り当てるユーザロールによって決定されます。たとえば、次のようになります。

- ユーザアカウントに **Manager** のユーザロールを割り当てる場合、ユーザは、関連のパーティション内のオブジェクト（ユーザアカウントオブジェクトは除く）に関するすべてのタスク（オブジェクトの作成、変更、削除など）を実行できます。
- ユーザアカウントに **Operator** のユーザロールを割り当てる場合、ユーザは、割り当てられたパーティション内にあるノードおよびプールメンバの有効化および無効化が制限されます。
- ユーザアカウントに **Guest** のユーザロールを割り当てる場合、ユーザは、パーティション内のオブジェクトの表示のみができます。割り当てられたパーティション内でのオブジェクトの作成、変更、削除はできません。

パーティションに対するユーザアクセスの設定は、ユーザアカウントを最初に作成したとき、またはユーザアカウントのプロパティを変更するときに行えます。以下の手順は、既存のユーザアカウントに対するパーティションアクセスの設定方法を示します。

◆注

*この手順は、ローカルユーザアカウントのみに関連します。リモートユーザアカウントに対するパーティションアクセスの設定については、『**TMOS™ Management Guide for BIG-IP® Systems**』を参照してください。*

パーティションのユーザアクセスを設定するには

1. ナビゲーションペインの [Main] タブで、[**System**] を展開して [**Users**] をクリックします。
   [User List] 画面が開きます。
2. [Name] カラムで、ユーザアカウント名をクリックします。
   そのユーザアカウントのプロパティ画面が開きます。
3. **No Access** 以外のアクセスレベルを付与するには、[**Role**] 設定を使用してユーザロールを選択します。

4. [**Partition Access**] リストからパーティション名を選択します。パーティション名を 1 つ選択するか、**All** を選択することができます。

   ***注 : Administrator** ロールを割り当てるユーザアカウントでは、この値は自動的に **All** に設定されます。*

5. [**Finished**] をクリックします。

パーティション内のオブジェクトの表示、管理、作成

管理ユーザが BIG-IP にログインし、BIG-IP システムオブジェクトの表示、管理、または作成を試みるときの動作を理解することは重要です。

システムオブジェクトの表示と管理

ユーザアカウントにユーザロールとパーティションを割り当てると、それらのユーザには、それらのユーザにアクセス権限が付与され BIG-IP オブジェクトのみが表示されます。ユーザは、それらのオブジェクトのみを表示でき、その他のオブジェクトは表示できません。

たとえば、Jane Smith というユーザが **jsmith** というユーザアカウントでシステムにログインするとします。また、このユーザは **Manager** のロールが割り当てられており、パーティション **A** の管理が許可されているとします。その場合、このユーザは、パーティション **A** に含まれるすべてのオブジェクト（ユーザアカウントオブジェクトも含む）の表示と管理ができるほか、パーティション **Common** 内のオブジェクトの表示ができます。このユーザは、システムの他のオブジェクトにはアクセスできません。すなわち、このユーザは設定ユーティリティを使用してシステム上のバーチャルサーバの一覧を表示する場合、パーティション **A** に含まれるバーチャルサーバの表示と管理ができるとともに、パーティション **Common** の任意のバーチャルサーバ（存在する場合）の表示ができることになります。また、このユーザはプールの一覧を表示する場合、パーティション **A** に含まれるプールの表示と管理を行うことができるとともに、パーティション **Common** の任意のプール（存在する場合）の表示ができ、他のオブジェクトの場合も同様です。このユーザは、別のパーティション内のオブジェクトへのアクセス（Read アクセスおよび Write アクセス）権限は持ちません。

一方、**Administrator** などのロールが割り当てられたユーザは、オブジェクトが配置されたパーティションとは無関係に、システム上のすべてのオブジェクトの表示および管理ができます。また、このタイプのロールが割り当てられたユーザは、表示や管理を行う特定パーティションを積極的に選択することもできます。

BIG-IP システムオブジェクトの作成

BIG-IP オブジェクトを特定のパーティションで作成する許可を付与するユーザロールが BIG-IP ユーザに割り当てられた場合、そのユーザが作成するオブジェクトは、そのユーザに管理が許可されたパーティション内に自動的に配置されます。

たとえば、Barry Jones にはユーザアカウント **bjones** が割り当てられており、このユーザアカウントはパーティション **B** の管理が許可されているとします。Barry が **bjones** アカウントを使用して BIG-IP にログインすると、このユーザが作成するオブジェクトはすべて、自動的にパーティション **B** に配置されます。

一方、オブジェクトの作成が許可されないロール（**Operator** ロールなど）が割り当てられたユーザがシステムにログインした場合、設定ユーティリティの画面に **[Create]** ボタンは表示されません。

ログインしたユーザがユニバーサルアクセス権限を持つ場合（**Administrator** ロールが割り当てられたユーザなど）、このユーザは BIG-IP オブジェクトの表示、管理、作成を行うパーティションを積極的に選択できます。

24

管理トラフィックのリモート認証および承認の設定

- BIG-IP ユーザアカウントのリモート認証と承認の 概要
- BIG-IP でユーザアカウントのリモート認証を使用 するための設定
- BIG-IP ユーザのアクセス制御の設定
- 複数の BIG-IP へのリモート認証データとリモート 承認データの伝播

BIG-IP ユーザアカウント のリモート 認証と 承認の概要

BIG-IP には、ネットワーク上の BIG-IP 管理アカウントを管理するための包括的なソリューションが用意されています。このソリューションには、以下の利点があります。

- **BIG-IP ユーザアカウントの管理にリモートサーバを使用できます。**
  BIG-IP は、リモート認証サーバによる BIG-IP ユーザアカウントの管理をサポートします。リモートサーバで BIG-IP システムアカウントを作成した後、ブラウザベースの設定ユーティリティまたはコマンドラインベースの **bigpipe** ユーティリティを使用して、リモートユーザ認証を使用するように BIG-IP を設定できます。詳細については、「*BIG-IP でユーザアカウントのリモート認証を使用 するための設定*」（24-2 ページ）を参照してください。
- **グループベースのアクセス制御を割り当てることができます。**
  BIG-IP には、**bigpipe** ユーティリティ内で使用できる **remoterole** マンドがあります。**remoterole** コマンドを使用して、リモートに保存された BIG-IP ユーザアカウントに対して、グループ全体を単位とするアクセス制御データを指定できます。**remoterole** コマンドでは、これらのリモートアカウントに割り当てられた既存のグループ定義を使用して、これらのユーザのアクセス制御プロパティ（特権）を定義することができます。**remoterole** コマンドにより、ユーザ特権の割り当ての精度と柔軟性が向上するだけでなく、これらの特権を割り当てる目的で BIG-IP 上のリモートユーザアカウントを複製する必要性がなくなります。
  詳細については、「*BIG-IP ユーザのアクセス制御の設定*」（24-6 ページ）を参照してください。
- **一連の認証データを複数の BIG-IP に伝播することができます。**
  BIG-IP には、ユーザアクセス制御データをネットワーク上の複数の BIG-IP に簡単に伝播できるツールがあります。このアクセス制御データには、ユーザロール指定、パーティションアクセス、BIG-IP コンソールアクセスなどが含まれます。ユーザ認証データを複数の BIG-IP に伝播するには、**bigpipe** ユーティリティ内のシングルコンフィグレーションファイル機能を使用します。詳細については、「*複数の BIG-IP へのリモート認証データとリモート 承認データの伝播*」（24-11 ページ）を参照してください。

上述の機能のすべてを組み合わせて使用することにより、グループ全体を単位としたユーザ特権の定義ができるとともに、BIG-IP ユーザアカウントを確実に管理できます。その結果、ネットワーク上の個別の BIG-IP ごとに独立したユーザアカウントを作成、管理する必要性がなくなります。

BIG-IP でユーザアカウント のリモート 認証を使用するための設定

リモートサーバ上のアカウントの作成が完了したら、BIG-IP がリモート認証サーバのタイプを指定するように設定する必要があります。これにより、BIG-IP ユーザを認証する際、BIG-IP がそのリモートデータにアクセスできるようになります。

BIG-IP は、BIG-IP 管理ユーザアカウントを保存するための認証サーバとして複数のタイプをサポートします。実際にユーザアカウントの保存に使用するリモートサーバタイプを指定する手順は、サーバのタイプによって異なります。

- LDAP（Lightweight Directory Access Protocol）サーバ
- Microsoft® Windows® Active Directory™ サーバ
- RADIUS（Remote Authentication Dial-in User Service）サーバ
- TACACS+（Terminal Access Controller Access-Control System Plus）サーバ

リモート LDAP サーバまたは Active Directory サーバの指定

BIG-IP では、BIG-IP のユーザアカウント、すなわち管理インタフェース（**MGMT**）を通過するトラフィックの認証に LDAP サーバまたは Microsoft Windows Active Directory サーバを使用するように設定することができます。

リモート認証サーバで SSL 認証トラフィックを認証するように設定する場合には、利用可能な追加機能がもう 1 つあります。クライアントトラフィックの認証時に通常はリモートサーバによって実行されるサーバ側の SSL ハンドシェイクを、BIG-IP が実行するように設定できます。その場合、SSL を使用したリモート認証の準備として事前に行う作業がいくつかあります。

SSL ベースのリモート認証を準備するには

BIG-IP 上で、設定ユーティリティを使用して証明書をインポートします。証明書のインポートについては、『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください。

SSL の準備作業が完了したら、次の「*リモート LDAP サーバまたは Active Directory サーバを指定するには*」の手順に従って SSL を有効にします。

リモート LDAP サーバまたは Active Directory サーバを指定するには

1. ナビゲーションペインの [Main] タブで [**System**] を展開し、[**Users**] をクリックします。
   [Users] 画面が開きます。
2. メニューバーで [**Authentication**] をクリックします。
   [Authentication] 画面が開きます。
3. [**Change**] をクリックします。

4. [**User Directory**] リストから [**Remote - Active Directory**] または [**Remote - LDAP**] を選択します。
5. [**Host**] ボックスに、リモートサーバの IP アドレスを入力します。
6. [**Port**] 設定では、デフォルトのポート番号（**389**）をそのまま使用するか、新しいポート番号をボックスに入力します。
この設定のポート番号は、BIG-IP がリモートサーバにアクセスする際に使用するポート番号です。
7. [**Remote Directory Tree**] ボックスに、LDAP または Active Directory サーバ上のユーザ認証データベースのファイルの位置（ツリー）を入力します。最低でもドメインコンポーネント（すなわち、**dc=<value>**）を指定する必要があります。
8. [**Scope**] 設定では、デフォルト値（**Sub**）をそのまま使用するか、新しい値を選択します。
この設定は、ユーザ認証時に BIG-IP が検索するリモートサーバデータベースのレベルを定義します。この設定に関する詳細については、オンラインヘルプを参照してください。
9. [**Bind**] 設定で、リモートサーバのユーザ ID ログインを指定します。
   a) [**DN**] ボックスに、リモートユーザ ID の識別名を入力します。
   b) [**Password**] ボックスに、リモートユーザ ID のパスワードを入力します。
   c) [**Confirm**] には、[Password] ボックスに入力したパスワードをもう一度入力します。
10. SSL ベースの認証を有効にする場合、[**SSL**] をクリックし、必要に応じて次の項目を設定します。
重要：*BIG-IP 上の保存場所を必ずフルパスで指定してください。たとえば、証明書がディレクトリ* ***/config/ssl/ssl.crt*** *に保存されている場合、値* ***/config/ssl/ssl.crt*** *を入力します。*
   a) [**SSL CA Certificate**] ボックスに、チェーン証明書、つまり、リモート認証サーバ上に通常存在するサードパーティ CA の証明書または自己署名証明書の名前を入力します。
   b) **[SSL Client Key] ボックスに、クライアント SSL キーの名前を入力します。**
この設定は、リモートサーバがクライアントに証明書の提示を要求する場合のみに使用します。クライアントの証明書が不要の場合には、この項目を設定する必要はありません。
   c) [**SSL Client Certificate**] ボックスに、**クライアント SSL 証明書の名前を入力します。**
この設定は、リモートサーバがクライアントに証明書の提示を要求する場合のみに使用します。クライアントの証明書が不要の場合には、この項目を設定する必要はありません。
11. [**Finished**] をクリックします。

リモート RADIUS サーバの指定

BIG-IP では、BIG-IP のユーザアカウント、すなわち管理インタフェース（**MGMT**）を通過するトラフィックの認証に RADIUS サーバを使用するように設定することができます。

リモート RADIUS サーバを指定するには

1. ナビゲーションペインの [Main] タブで [**System**] を展開し、[**Users**] をクリックします。
   [Users] 画面が開きます。
2. メニューバーで [**Authentication**] をクリックします。
   [Authentication] 画面が開きます。
3. [**Change**] をクリックします。
4. [**User Directory**] リストから [**Remote - RADIUS**] を選択します。
5. [**Server Configuration**] リストから、[**Primary Only**] または [**Primary & Secondary**] を選択します。
6. [**Primary**] 設定で、以下の項目を設定します。
   a) [**Host**] ボックスに、リモートサーバの IP アドレスを入力します。
   b) [**Port**] ボックスでは、デフォルトのポート番号（**1812**）をそのまま使用するか、新しいポート番号をボックスに入力します。
   この設定のポート番号は、BIG-IP がリモートサーバにアクセスする際に使用するポート番号です。
   c) [**Secret**] ボックスに、RADIUS シークレットを入力します。
   d) [**Confirm**] ボックスに、[**Secret**] ボックスで入力したシークレットをもう一度入力します。
   [**Secret**] 設定の値と [**Confirm**] 設定の値が一致しなければなりません。
7. 手順 5 で [**Primary & Secondary**] を選択した場合には、[**Secondary**] を設定します。
8. [**Finished**] をクリックします。

TACACS+ サーバの指定

BIG-IP では、BIG-IP のユーザアカウント、すなわち管理インタフェース（**MGMT**）を通過するトラフィックの認証に TACACS+ サーバを使用するように設定することができます。

リモート TACACS+ 認証を設定するには

1. ナビゲーションペインの [Main] タブで [**System**] を展開し、[**Users**] をクリックします。
   [Users] 画面が開きます。
2. メニューバーで [**Authentication**] をクリックします。
   [Authentication] 画面が開きます。

3. [**Change**] をクリックします。
4. [**User Directory**] リストから [**Remote - TACACS+**] を選択します。
5. [**Configuration**] リストから、[**Advanced**] を選択します。
画面に追加設定が表示されます。
6. [**Servers**] ボックスに IP アドレスを入力し、[**Add**] をクリックします。
7. [**Secret**] ボックスに、TACACS+ のシークレットを入力します。
8. [**Confirm Secret**] ボックスに、[**Secret**] ボックスで入力した TACACS+ シークレットをもう一度入力します。
9. [**Encryption**] リストでは、デフォルト値（[**Enabled**]）をそのまま使用するか、リストから [**Disabled**] を選択します。この設定はオプションです。
10. [**Service Name**] ボックスに、サービスの名前を入力します。
11. [**Protocol Name**] ボックスに、プロトコルの名前を入力します。この設定はオプションです。
12. [**Authentication**] リストから、[**Authenticate to first server**] または [**Authenticate to each server until success**] を選択します。
13. [**Accounting Information**] リストから、[**Send to first available server**] または [**Send to all servers**] を選択します。
14. [**Debug Logging**] リストから、[**Disabled**] または [**Enabled**] を選択します。
15. [**Finished**] をクリックします。

BIG-IP ユーザのアクセス制御の設定

ユーザアカウントの保存に使用しているリモートサーバのタイプを指定した後、これらのアカウントの承認プロパティ（すなわち、ユーザロール、パーティションアクセス、ターミナルアクセス）の設定ができます。

BIG-IP ユーザアカウントを保存するために使用されているリモートサーバのタイプを示すように BIG-IP を設定した場合、BIG-IP は、リモートで保存されたアカウントのすべてを表す単一ユーザエンティティを自動的にBIG-IP上に作成しています。このユーザエンティティは **Other External Users** と呼ばれ、ここにはデフォルトのアクセス制御値が含まれます。これらのアクセス制御値は以下のとおりです。

- Role = **No Access**
- Partition = **All**
- Terminal Access = **Disabled**

◆注

設定ユーティリティを使用して、リモートユーザアカウントに特権を割り当てる際に BIG-IP がデフォルトとして使用する値を変更できます。

Other External Users で表されるユーザアカウントのすべてに対してデフォルト以外の値を使用する場合は、以下の 2 つの選択肢があります。

- **remoterole コマンドを使用する（推奨）。**
  これにより、特権をグループ単位で割り当てることができます。**remoterole** コマンドを使用する場合、リモートユーザアカウントによる BIG-IP システムリソースのアクセスを制御する際の柔軟性と精度が向上します。詳細については、このページの「*remoterole コマンドの概要*」を参照してください。
- **設定ユーティリティを使用してユーザごとに特権を割り当てる。**
  設定ユーティリティを使用する場合、リモートに保存された個々のユーザアカウントにデフォルト以外の特権を割り当てることができます。その場合には、最初に BIG-IP 上のユーザアカウントを複製する必要があります。詳細については、『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください。

◆注

*アカウントに割り当てることができるユーザロールの詳細については、『**TMOS™ Management Guide for BIG-IP® Systems**』を参照してください。*

remoterole コマンドの概要

remoterole コマンドは、定義するアクセス制御プロパティにベンダ固有の属性（ユーザグループを定義するための LDAP 属性など）をマッピングすることにより、リモートユーザアカウントに特権を割り当てます。これらのアクセス制御プロパティは以下のとおりです。

- ユーザロール
- コンソールアクセスまたは制限
- ユーザパーティション割り当て

リモート認証サーバ属性をアクセス制御プロパティにマッピングすることにより、リモート認証サーバに保存された BIG-IP ユーザアカウントのグループごとに、アクセス制御プロパティのさまざまなセットを簡単に定義できます。

remoterole コマンドを使用しない場合、リモートに保存されたすべてのユーザアカウントに同じ特権を割り当てるか、BIG-IP 上の各リモートユーザアカウントを個別に複製して、固有の特権をそのアカウントに割り当てる必要があります。

remoterole ユーティリティを使用した場合、シングルコンフィグレーションファイル機能を使用して、そのアクセス制御データをネットワーク上の他の BIG-IP に伝播することができます。詳細については、「*複数の BIG-IP へのリモート認証データとリモート 承認データの伝播*」（24-11 ページ）を参照してください。

remoterole コマンドの使用

グループ全体の特権をリモートユーザアカウントに割り当てるには、**remoterole** コマンドを使用します。このコマンドは、**bigpipe** ユーティリティから利用できます。ここでは、**remoterole** コマンドの構文と使用例、およびその結果として設定されるアクセス制御データを示します。

リモートユーザアカウントに特権を割り当てるには

以下の構文を使用して、**bigpipe remoterole** コマンドを入力します。

```
bigpipe remoterole role info <user group> attribute (<string> | none) console \
    (enable | disable) line order <number> role <user role> user partition \
    (<string> | none)
```

たとえば、BIG-IP ユーザアカウントが LDAP リモート認証サーバに保存されており、これらのアカウントは **BigIPOperatorsGroup** と **BigIPManagersGroup** のグループに分割されているとします。この場合、以下の **remoterole** コマンドシーケンスを入力することにより、これらのグループの特権を定義できます。

```
bigpipe remoterole role info BigIPOperatorsGroup { attribute
    "memberOF=cn=BigIPOperatorsGroup,cn=users,dc=dev,dc=net" console disable line order 1
    role operator user partition App_A } role info BigIPManagersGroup { attribute
    "MemberOF=cn=BigIPManagersGroup,cn=users,dc=dev,dc=net" console enable line order 2
    role manager user partition App_B }
```

表 24.1 は、コマンドの結果として、それぞれのグループに割り当てられる特権を示します。

グループ名	割り当てられる特権
BigIPOperatorsGroup	**console** disable **role** operator **user partition** App_A
BigIPManagersGroup	**console** enable **role** manager **user partition** App_B

***表 24.1 remoterole** コマンドの結果として割り当てられる特権*

◆注

***remoterole** コマンドを使用してグループベースの特権を設定した後、リモートサーバ上のグループ割り当てを持たないユーザが BIG-IP にログオンすると、BIG-IP へのアクセスが拒否されます。また、リモートアカウントのユーザロールまたはパーティション割り当て(あるいはその両方)を変更すると必ず、**Other External Users** としてログインしたユーザも含め、すべてのユーザは即座にシステムからログオフされます。*

変数置換の使用

BIG-IP 環境によっては、膨大な数の管理パーティションとユーザロールを使用する場合があり、ユーザロールとパーティションの異なる組み合わせがいくつか必要になります。たとえば、BIG-IP が 10 個の管理パーティションと5個のユーザロールを使用するように設定されている場合、BIG-IP では 50 個のユーザロールとパーティションの異なる組み合わせが必要になる可能性があります。その場合に **remoterole** コマンドで処理するのは手間がかかります。

この問題を軽減するために、**remoterole** コマンドは、変数置換をサポートします。すなわち、**remoterole** コマンドの引数 **role**、**user partition**、**console** に対し、値の **%<variable>** 変数を指定することができます。

例

リモート RADIUS 認証サーバがベンダ固有の属性と 3 つの変数、およびその値を返すように設定されているとします。

- F5-LTM-User-Info-1 = **DC1**
- F5-LTM-User-Role = **400**
  注 : 詳細については、「*変数評価の考慮事項*」（24-9 ページ）を参照してください。
- F5-LTM-User-Partition = **App_C**
- F5-LTM-User-Console = **1**

remoterole コマンドは、一致の検索用に最初の属性（**F5-LTM-User-Info-1**）を使用できます。そして、コマンドは、**role**、**user partition**、**console** の値を残りの 3 つの変数から読み出すことができます。したがって、これらを明示的に指定する必要がありません。コマンドでこのように使用するには、これら 3 つの変数を、それぞれの前に文字列 **%** を付け、引数としてコマンドラインに指定します。

remoterole コマンドの使用例を以下に示します。このコマンドは、ベンダ固有の属性 **F5-LTM-User-Info-1** の一致を検索し、上述のアクセス制御値（**Operator**、**App_C**、**1**）を Datacenter 1（**DC1**）に属するユーザアカウントに割り当てます。

```
b remoterole role info DC1 { attribute "F5-LTM-User-Info-1=DC1"
    console "%F5-LTM-User-Console" role "%F5-LTM-User-Role" user partition
    "%F5-LTM-User-Partition" line order 1 }
```

変数評価の考慮事項

変数置換を remoterole コマンドで使用する場合、BIG-IP は以下のルールに従うため、これらを考慮する必要があります。

- **不適切な変数値**
  変数の値が不適切な場合、ユーザは承認されません。たとえば、**%F5-LTM-User-Partition** 変数が **p1** に評価される場合において、**p1** パーティションが存在しないか、このパーティションの名前が **p1** ではなく、**P1** の場合、ユーザはログインしようとするとエラーメッセージを受け取ります。
- **role 変数**
  コマンドラインで指定した変数が **role** 引数（たとえば、**%F5-LTM-User-Role**）を持つ場合、この変数は以下のいずれかに評価される必要があります。
  - **0** (**Administrator**)
  - **20** (**Resource Administrator**)
  - **40** (**User Manager**)
  - **100** (**Manager**)
  - **300** (**Application Editor**)
  - **400** (**Operator**)
  - **700** (**Guest**)
  - **800** (**Application Security Policy Editor**)
  - **900** (**None**)
- **変数の不足**
  認証属性に変数が不足している場合、BIG-IP は以下の特権をユーザアカウントに割り当てます。
  - Role = **No Access**
  - Partition = **None**
  - Terminal access = **Disabled**

- **属性の不一致**
  ユーザは正しく認証されたが、**remoterole** 属性のいずれにも一致しない場合、BIG-IP はデフォルトの特権を割り当てます。リモートユーザのデフォルトの特権については、「*BIG-IP ユーザのアクセス制御の設定*」（24-6 ページ）を参照してください。

複数のBIG-IPへのリモート 認証データとリモート承認データの伝播

BIG-IP 管理ユーザのリモート認証および承認を設定するための最後の手順では、BIG-IP 認証および承認のデータをネットワーク上の BIG-IP に伝播します。

この手順の実行には、単一設定ファイル機能に含まれる **bigpipe export** コマンドおよび **bigpipe import** コマンドを使用します。**bigpipe export** コマンドは、BIG-IP 設定データを特別な **.scf** ファイル（SCF）ファイルにエクスポートします。**bigpipe import** コマンドは、その SCF 内のデータを使用して、他の BIG-IP を設定します。

上述のタスク（**remoterole** コマンドによるリモートユーザアカウントのアクセス制御データの定義）を実行した場合、それ以降に **bigpipe export** コマンドを使用して作成するすべての SCF には、それらのアクセス制御定義が含まれます。その場合には、**bigpipe import** コマンドを使用して、そのアクセス制御データをネットワーク上の他の BIG-IP に伝播することができます。

以下の手順は、SCF の作成方法と、SCF を別の BIG-IP にインポートする方法を示します。SCF の機能とその使用方法の詳細については、『***TMOS*™ *Management Guide for BIG-IP*® *Systems***』を参照してください。

SCF を作成するには

1. **bigpipe** シェルをアクセスします。
2. **export** コマンドを実行し、SCF の名前を指定します。たとえば、以下のようにします。

   ```
   bp> export myConfiguration053107
   ```

   /var/local/scf ディレクトリにファイル **myConfiguration053107.scf** が作成されます。別の場所に SCF を作成する場合は、ファイルのフルパスを指定してください。たとえば、**export /config/myConfiguration** コマンドは、SCF を **/config** ディレクトリに作成します。

SCF を使用して別の BIG-IP を設定するには

1. 上述のセクションで作成した CSF を、設定する BIG-IP からアクセス可能なネットワーク上の場所にコピーします。
2. 設定する BIG-IP の管理ルーティングと特別なパスワードを反映するように SCF を編集します。

   a) SCF をエディタで開きます。

   b) 必要に応じて、管理 IP アドレス、ネットワークマスク、管理デフォルトルート、セルフ IP アドレス、バーチャルサーバ IP アドレス、ルート、デフォルトルート、およびホスト名のフィールドの値を新しいシステムの値に変更します。

c) 必要に応じて、**root** および **admin** アカウントのパスワードを、**user <name> password none newpassword <password>** コマンドで変更します。
重要：*冗長システムの一部となるユニットを、SCF を使用してシステム内の別のユニットから設定する場合、**root** アカウントおよび**admin** アカウントは変更しないでください。これらのアカウントは、冗長システムの両方のユニットで同じでなければなりません。*

d) 編集した SCF を保存します。

3. 設定する BIG-IP で、**import** コマンドを使用して SCF をインポートします。

```
bp> import myConfiguration
```

BIG-IP は、実行設定のコピーを **/var/local/scf** ディレクトリに保存した後、この実行設定をインポートした SCF が含まれる設定でリセットします。

4. 新しい実行設定を保存済みの設定に保存するには、**save all** コマンドを使用します。
BIG-IP は、新しい実行設定を保存済みの設定に保存します。

25

アプリケーショントラフィックのリモート認証の設定

- アプリケーショントラフィックのリモート認証の概要
- リモート LDAP サーバまたは Active Directory サーバを使用する認証の設定
- リモート RADIUS サーバを使用する認証の設定
- リモートTACACS+サーバを使用する認証の設定
- リモート LDAP サーバを使用した SSL ベースの承認の設定
- OCSP レスポンダを使用した SSL 証明書失効の設定
- CRLDP 認証モジュールの設定

アプリケーショントラフィックのリモート認証の概要

大規模なコンピューティング環境の管理者は、自社のユーザアカウントを専用の認証サーバにリモートから保存することを好みます。BIG-IP を設定することにより、この認証サーバを使用して、BIG-IP を通過するすべてのネットワークトラフィックを認証することが可能になります。通常、リモート認証サーバは、以下のプロトコルを使用します。

- LDAP（Lightweight Directory Access Protocol）
- RADIUS（Remote Authentication Dial-In User Service）
- TACACS+ (derived from Terminal Access Controller Access Control System [TACACS])
- OCSP（Online Certificate Status Protocol）
- Certificate Revocation List Distribution Point (CRLDP)

リモート認証サーバを使用することにより、BIG-IP では、以下の 2 タイプのネットワークトラフィックの認証ができます。

- **ロードバランシングされるアプリケーショントラフィック**
  このタイプのトラフィックは、バーチャルサーバを通過し、さらに TMM（Traffic Management Microkernel）インターフェイスを通過します。このタイプのトラフィックにリモート認証を設定するには、ユーザアカウントの保存に使用する認証サーバのタイプに対応した構成オブジェクトとプロファイルを作成する必要があります。たとえば、リモート認証サーバが LDAP サーバの場合、LDAP 構成オブジェクトと LDAP プロファイルを作成します。これらの作業の詳細については、この章の後の説明、設定ユーティリティの [Help] タブまたは『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。
- **BIG-IP 管理用の管理トラフィック**
  このタイプのトラフィックは、バーチャルサーバを通過しませんが、その代わりに管理インターフェイス（MGMT）を通過します。このタイプのトラフィックにリモート認証を設定する場合には、管理ユーザアカウントを作成します。詳細については、本ガイドの第 24 章「*管理トラフィックのリモート認証および承認の設定*」および『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください。

BIG-IP を通過するアプリケーショントラフィックの認証にリモートサーバを使用する場合、以下のサーバタイプのいずれかを選択できます。

- LDAP サーバまたは Active Directory サーバ
- RADIUS サーバ
- TACACS+ サーバ
- SSL OCSP レスポンダ
- CRLDP サーバ
- Kerberos サーバ

アプリケーショントラフィックに対してリモートユーザ認証を設定するには、構成オブジェクトと認証プロファイルの両方を作成する必要があります。それぞれの認証サーバタイプには、異なる構成オブジェクトとプロファイルが必要です。たとえば、LDAP 認証サーバを使用するように BIG-IP を設定するには、LDAP 構成オブジェクトとカスタム LDAP プロファイルを作成する必要があります。

RADIUS、SSL OCSP または CRLDP タイプの認証モジュールを実装する場合には、また別のタイプのオブジェクトを作成する必要があります。RADIUS および CRLDP 認証の場合、このオブジェクトは、***サーバオブジェクト***と呼ばれます。SSL OCSP 認証の場合、このオブジェクトとは、***OCSP レスポンダ***と呼ばれます。

◆注

*Kerberos 認証の設定については、第 26 章「**Kerberos 委任の設定**」を参照してください。*

リモート LDAP サーバまたは Active Directory サーバを使用する認証の設定

BIG-IP では、BIG-IP の TMM インターフェイスを通過するトラフィックの認証に LDAP サーバまたは Active Directory サーバを使用するように設定することができます。デフォルトでは、クライアントの資格情報はベーシック HTTP 認証（つまりユーザ名とパスワード）に基づきます。ただし、SSL キーと証明書に基づく SSL 認証を有効にすることもできます。

アプリケーショントラフィックに対して LDAP 認証または Active Directory 認証を設定するには、次の作業を完了します。

- LDAP タイプの構成オブジェクトを作成する
- LDAP タイプの認証プロファイルを作成する
- HTTP トラフィックの管理用に構成されたバーチャルサーバを変更する

LDAP 構成オブジェクトの作成

BIG-IP で LDAP ベースまたは Active Directory ベースのリモート認証を設定するには、最初に、設定ユーティリティを使用してカスタム LADP 構成オブジェクトを作成してください。***LDAP 構成オブジェクト***では、BIG-IP がリモート認証を実行するために必要な情報を指定します。たとえば、システムが認証データのソースロケーションとして使用するリモート LDAP ツリーを LDAP 構成オブジェクトで指定します。

リモート認証サーバで LDAP または Active Directory を使用し、SSL 認証トラフィックを認証するように設定する場合には、利用可能な追加機能がもう 1 つあります。クライアントトラフィックの認証時に通常はリモート サーバによって実行される、サーバ側の SSL ハンドシェイクを

実行するように BIG-IP を設定できます。この場合には、SSL を使用したリモート認証を準備するための予備的な作業をいくつか実行する必要があります。

SSL ベースのリモート認証を準備するには

1. 認証局（CA）または自己署名の証明書を PEM 形式に変換します。
2. BIG-IP で、設定ユーティリティを使用して証明書をインポートします。
   証明書は、BIG-IP の任意の場所に保存できます。

これらの SSL の予備作業を完了したら、SSL ベースのリモートサーバ認証を有効にすることができます。この作業は、LDAP 構成オブジェクト作成の一部です。この構成オブジェクトには、以下の詳細設定があります。

- **SSL CA Certificate**
  リモート認証サーバに通常ある証明書の名前を示します。
- **SSL Client Key**
  クライアントが BIG-IP に送信する SSL キーの名前を示します。このキーの指定は、リモートサーバがクライアント証明書を要求する場合にのみ必要です。
- **SSL Client Certificate**
  クライアントが BIG-IP に送信する SSL 証明書の名前を示します。この証明書の指定は、リモートサーバがクライアント証明書を要求する場合にのみ必要です。

◆ 重要

*LDAP 構成オブジェクトの作成中にキーファイルや証明書ファイルを指定する場合には、BIG-IP 上の保存場所を必ずフルパス名で指定してください。たとえば、証明書がディレクトリ **/config/ssl/ssl.crt** に保存されている場合、値 **/config/ssl/ssl.crt** を入力します。*

カスタム LDAP 構成オブジェクトを作成したら、カスタム LDAP プロファイルを作成し、このカスタムプロファイルを HTTP バーチャルサーバに割り当てます。

カスタム LDAP 構成オブジェクトの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. [Authentication] メニューの [Configurations] を選択します。
   [Authentication Configurations] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
   [New Authentication Configuration] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールでは LDAP 構成オブジェクトを作成する権限が与えられていないことを示します。*

4. [**Name**] ボックスに、構成オブジェクトに一意の名前（**my_ldap_config** など）を入力します。
5. [**Type**] リストから、[**LDAP**] を選択します。
これで、ユーザ設定可能な構成オブジェクト設定が表示されます。
6. [Configuration] 領域では、[**Basic**] または [**Advanced**] を選択します。
[**Advanced**] を選択した場合、追加の設定項目が画面に表示されます。
7. [**Remote LDAP Tree**] ボックスに、LDAP または Active Directory サーバ上のユーザ認証データベースのファイルの位置（ツリー）を入力します。
最低でもドメインコンポーネント（すなわち、**dc=<value>**）を指定する必要があります。
8. [**Hosts**] 設定で、次の作業を行います。
   a) リモート LDAP サーバまたは Active Directory サーバの IP アドレスを入力します。
   b) [**Add**] をクリックします。
   IP アドレスがテキストウィンドウに表示されます。
9. [**Service Port**] の値をそのまま使用するか変更します。
10. [**LDAP Version**] の値をそのまま使用するか変更します。
11. 手順 6 で基本的な構成を選択した場合は、[**Finished**] をクリックします。手順 6 で詳細な構成を選択した場合は、残りの設定を継続し、[**Finished**] をクリックします。

◆注

*SSL 認証の有効化については、この項の冒頭の「**LDAP 構成オブジェクトの作成**」(25-2 ページ）を参照してください。*

LDAP 認証プロファイルの作成

BIG-IP で LDAP ベースまたは Active Directory ベースのリモート認証を設定する次の作業は、カスタム LADP プロファイルの作成です。***LDAP プロファイル***では、LDAP 認証モード（[**Enabled**] または [**Disabled**]）、先に作成した LDAP 構成オブジェクトの名前などの情報を指定します。

カスタム LDAP プロファイルを作成したら、このカスタムプロファイルとデフォルトの iRule をバーチャルサーバに割り当てます。

カスタム LDAP プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. [Authentication] メニューの [Profiles] を選択します。
   [Authentication Profiles] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
   [New Authentication Profile] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールでは LDAP プロファイルを作成する権限が与えられていないことを示します。*
4. [**Name**] ボックスに、プロファイルに一意の名前（**my_ldap_profile** など）を入力します。
5. [**Type**] リストから、[**LDAP**] を選択します。
   これで、ユーザ設定可能なプロファイル設定が表示されます。
6. [**Parent Profile**] リストで [**ldap**] が選択されていることを確認します。
   これで、**ldap** という名前のデフォルトプロファイルからデフォルトの構成値が新しいプロファイルに継承されます。
7. [**Configuration**] リストから、先に作成した LDAP 構成オブジェクトの名前を選択します。
8. 残りの設定はすべて、デフォルト値をそのまま使用します。
9. [**Finished**] をクリックします。

LDAP 認証用バーチャルサーバの変更

リモート LDAP サーバによる認証の実装プロセスでの最後の作業は、カスタム LDAP プロファイルとデフォルトの LDAP 認証 iRule を、HTTP トラフィック処理用に構成されたバーチャルサーバ（すなわち、HTTP プロファイルが割り当てられたバーチャルサーバ）に割り当てる作業です。

◆注

プロファイルと iRule を割り当てるバーチャルサーバは、標準タイプのバーチャルサーバでなければなりません。

LDAP 認証用バーチャルサーバの変更方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. Name カラムで、HTTP プロファイルを割り当てる標準タイプバーチャルサーバの名前をクリックします。
   選択したバーチャルサーバのプロパティが表示されます。
3. [**Configuration**] リストから、[**Advanced**] を選択します。
   その他のプロパティが表示されます。
4. [**Authentication Profiles**] リストの [**Available**] ボックスで、先に作成したカスタム LDAP プロファイルの名前を選択し、Move ボタン（<<）をクリックします。
   選択したプロファイル名が [**Enabled**] ボックスに移動します。

   注 : [Authentication Profiles] *リストを変更できない場合は、現在のユーザロールではバーチャルサーバを変更する権限が与えられていないことを示します。*
5. [**Update**] をクリックします。

リモート RADIUS サーバを使用する認証の設定

RADIUS 認証モジュールとは、BIG-IP 経由のクライアント接続を認証するための機構です。このモジュールは、リモート RADIUS サーバに認証データが格納されている場合に使用します。この場合、クライアントの資格情報はベーシック HTTP 認証（つまりユーザ名とパスワード）に基づきます。

RADIUS 認証モジュールを実装するには、リモート RADIUS サーバ上のデータにアクセスするようにBIG-IPを設定する必要があります。このために、次の作業を行う必要があります。

- 1 つ以上の上位 RADIUS サーバオブジェクトを作成する
- RADIUS 構成オブジェクトを作成する
- RADIUS プロファイルを作成する
- バーチャルサーバを変更し、RADIUSプロファイルをそのバーチャルサーバへ割り当てる

RADIUS サーバオブジェクトの作成

BIG-IP で RADIUS ベースのリモート認証を設定するには、最初に、カスタム RADIUS サーバオブジェクトを作成してください。カスタム RADIUS サーバオブジェクトを作成したら、カスタム RADIUS 構成オブジェクトとカスタム RADIUS プロファイルを作成し、このカスタムプロファイルとデフォルトの iRule を HTTP バーチャルサーバに割り当てます。

RADIUS サーバオブジェクトを作成するには

1. ナビゲーションページの Main タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [Profiles] 画面が開きます。
2. [Authentication] メニューの [RADIUS Servers] を選択します。
   [RADIUS Server List] 画面が表示されます。
3. 画面の右上で [**Create**] をクリックします。
   [RADIUS Server] 画面が表示されます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールでは RADIUS サーバオブジェクトを作成する権限が与えられていないことを示します。*
4. **my_radius_server** など、RADIUS サーバオブジェクトの一意の名前を [**Name**] 設定に入力します。
5. [**Server**] 設定にリモート RADIUS サーバのホスト名または IP アドレスを入力します。
6. [**Secret**] 設定と [**Confirm Secret**] 設定に「RADIUS secret」と入力します。
7. デフォルトの [**Timeout**] の値をそのまま使用します。
8. [**Finished**] をクリックします。

RADIUS 構成オブジェクトの作成

BIG-IP で RADIUS ベースのリモート認証を設定する次の作業は、カスタム RADIUS 構成オブジェクトの作成です。***RADIUS 構成オブジェクト***では、BIG-IP がリモート認証を実行するために必要な情報を指定します。

カスタム RADIUS 構成オブジェクトを作成したら、カスタム RADIUS プロファイルを作成し、このカスタムプロファイルを HTTP バーチャルサーバに割り当てます。

RADIUS 構成オブジェクトを作成するには

1. [Main] タブで [**Local Traffic**] を展開し、[**Profiles**] をクリックします。
   [Profiles] 画面が開きます。
2. [**Authentication**] メニューの [**Configurations**] を選択します。
   [Authentication Configurations] 画面が表示されます。
3. 画面の右上で [**Create**] をクリックします。
   [New Authentication Configuration] 画面が表示されます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールでは RADIUS 構成オブジェクトを作成する権限が与えられていないことを示します。
4. [**Name**] 設定に、構成オブジェクトに一意の名前（**my_radius_config** など）を入力します。
5. [**Type**] 設定から [**RADIUS**] を選択します。
   画面が拡張され、いくつかの設定が表示されます。
6. [**Configuration**] リストから、[**Basic**] または [**Advanced**] を選択します。
   [**Advanced**] を選択した場合、追加の設定項目が画面に表示されます。
7. [**RADIUS Servers**] 設定の [**Available**] ボックスから、RADIUS サーバの IP アドレスを選択し、Move ボタン（<<）をクリックします。
   選択したサーバ名が [**Selected**] ボックスに移動します。
8. [**Client ID**] ボックスに文字列で **NAS-Identifier** と入力します。
   RADIUS 認証が要求されると、**NAS-Identifier** 文字列はアクセス要求パケットに含められ、パケット送信元の NAS を特定します。**NAS-Identifier** 文字列の例としては、完全修飾ドメイン名（FQDN）が挙げられます。
9. 手順 7 で基本的な構成を選択した場合は、[**Finished**] をクリックします。手順 7 で詳細な構成を選択した場合は、残りの設定を継続し、[**Finished**] をクリックします。

RADIUS プロファイルの作成

BIG-IP で RADIUS ベースのリモート認証を設定する次の作業は、カスタム RADIUS プロファイルの作成です。***RADIUS プロファイル***では、RADIUS 認証モード（[**Enabled**] または [**Disabled**]）、先に作成した RADIUS 構成オブジェクトの名前などの情報を指定します。

プロファイルを作成したら、このカスタムプロファイルとデフォルトの iRule をバーチャルサーバに割り当てます。

カスタム RADIUS プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. [Authentication] メニューの [Profiles] を選択します。
   [Authentication Profiles] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
   [New Authentication Profile] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールでは RADIUS プロファイルを作成する権限が与えられていないことを示します。*
4. [**Type**] リストから、[**RADIUS**] を選択します。
   これで、ユーザ設定可能なプロファイル設定が表示されます。
5. [**Name**] ボックスに、プロファイルに一意の名前（**my_radius_profile** など）を入力します。
6. [**Parent Profile**] リストで [**radius**] が選択されていることを確認します。
   これで、**radius** という名前のデフォルトプロファイルからデフォルトの構成値が新しいプロファイルに継承されます。
7. [**Configuration**] リストから、先に作成した RADIUS 構成オブジェクトの名前を選択します。
8. 残りの設定はすべて、デフォルト値をそのまま使用します。
9. [**Finished**] をクリックします。

RADIUS 認証用バーチャルサーバの変更

リモート RADIUS サーバによる認証の実装プロセスでの最後の作業は、カスタム RADIUS プロファイルを、HTTP トラフィック処理用に構成されたバーチャルサーバ（すなわち、HTTP プロファイルが割り当てられたバーチャルサーバ）に割り当てる作業です。

◆注

認証プロファイルを割り当てるバーチャルサーバは、標準タイプのバーチャルサーバでなければなりません。

RADIUS 認証用バーチャルサーバの変更方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. [Name] カラムで、バーチャルサーバの名前をクリックします。
   選択したバーチャルサーバのプロパティが表示されます。
3. [**Configuration**] リストから、[**Advanced**] を選択します。
   その他のプロパティが表示されます。
4. [**Authentication Profiles**] リストの [**Available**] ボックスで、先に作成したカスタム RADIUS プロファイルの名前を選択し、Move ボタン（<<）をクリックします。
   選択したプロファイル名が [**Enabled**] ボックスに移動します。

   注 : [Authentication Profiles] *リストを変更できない場合は、現在のユーザロールではバーチャルサーバを変更する権限が与えられていないことを示します。*
5. [**Update**] をクリックします。

リモート TACACS+ サーバを使用する認証の設定

BIG-IP では、BIG-IP の TMM インターフェイスを通過するトラフィックの認証にTACACS+サーバを使用するように設定することができます。この場合、クライアントの資格情報はベーシック HTTP 認証（つまりユーザ名とパスワード）に基づきます。

アプリケーショントラフィックに対してTACACS+認証を設定するには、次の作業を完了します。

- TACACS+ タイプの構成オブジェクトを作成する
- TACACS+ タイプの認証プロファイルを作成する
- HTTPトラフィックの管理用に構成されたバーチャルサーバを変更する

TACACS+ 構成オブジェクトの作成

BIG-IP で TACACS+ リモート認証を設定するには、最初に、カスタム TACACS+ 構成オブジェクトを作成してください。TACACS+ ***構成オブジェクト***では、BIG-IP がリモート認証を実行するために必要な情報を指定します。たとえば、リモート TACACS+ サーバの IP アドレスなどを構成オブジェクトで指定します。

カスタム TACACS+ 構成オブジェクトの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. [Authentication] メニューの [Configurations] を選択します。
   [Authentication Configurations] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
   [New Authentication Configuration] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではTACACS+ 構成オブジェクトを作成する権限が与えられていないことを示します。*
4. [**Type**] リストから、[**TACACS+**] を選択します。
   これで、ユーザ設定可能な構成オブジェクト設定が表示されます。
5. [**Name**] ボックスに、構成オブジェクトに一意の名前（**my_tacacs_config** など）を入力します。
6. [Configuration] 領域では、[**Basic**] または [**Advanced**] を選択します。
   [**Advanced**] を選択した場合、追加の設定項目が画面に表示されます。
7. [**Servers**]ボックスにTACACS+サーバのIPアドレスを入力し、[**Add**] をクリックします。
   IP アドレスがテキストウィンドウに表示されます。

8. [**Hosts**] 設定で、リモート LDAP サーバまたは Active Directory サーバの IP アドレスを入力し、[**Add**] をクリックします。
IP アドレスがテキストウィンドウに表示されます。
9. サーバとの間で送受信されるパケットを暗号化または復号化するためのTACACS+秘密鍵を[**Secret**]ボックスに入力します。
10. [**Confirm Secret**] ボックスには、[**Secret**] ボックスに入力した秘密鍵をもう一度入力します。
11. 手順 6 で基本的な構成を選択した場合は、[**Finished**] をクリックします。手順 6 で詳細な構成を選択した場合は、残りの設定を継続し、[**Finished**] をクリックします。

TACACS+ 構成オブジェクトを作成したら、カスタム TACACS+ プロファイルを作成し、HTTPバーチャルサーバを変更する必要があります。

TACACS+ プロファイルの作成

BIG-IP で TACACS+ ベースのリモート認証を設定する次の作業は、カスタム TACACS+ プロファイルの作成です。プロファイルを作成したら、このカスタムプロファイルとデフォルトの **http** プロファイル、およびデフォルトの iRule をバーチャルサーバに割り当てます。

カスタム TACACS+ プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
[HTTP Profiles] 画面が開きます。
2. [Authentication] メニューの [Profiles] を選択します。
[Authentication Profiles] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
[New Authentication Profile] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではTACACS+ プロファイルを作成する権限が与えられていないことを示します。*
4. [**Type**] リストから、[**TACACS+**] を選択します。
これで、ユーザ設定可能なプロファイル設定が表示されます。
5. [**Name**] ボックスに、プロファイルに一意の名前（**my_tacacs_profile** など）を入力します。
6. [**Parent Profile**] リストで [**tacacs**] が選択されていることを確認します。
これで、**tacacs** という名前のデフォルトプロファイルからデフォルトの構成値が新しいプロファイルに継承されます。
7. [**Configuration**] リストから、先に作成した TACACS+ 構成オブジェクトの名前を選択します。
8. 残りの設定はすべて、デフォルト値をそのまま使用します。
9. [**Finished**] をクリックします。

TACACS+ 認証用バーチャルサーバの変更

リモートTACACS+サーバによる認証の実装プロセスでの最後の作業は、カスタム TACACS+ プロファイルと既存のデフォルト認証 iRule を、HTTP トラフィック処理用に構成されたバーチャルサーバ（すなわち、HTTP プロファイルが割り当てられたバーチャルサーバ）に割り当てる作業です。

◆注

認証プロファイルと iRule を割り当てるバーチャルサーバは、標準タイプのバーチャルサーバでなければなりません。

TACACS+ 認証用バーチャルサーバの変更方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. [Name] カラムで、バーチャルサーバの名前をクリックします。
   選択したバーチャルサーバのプロパティが表示されます。
3. [**Configuration**] リストから、[**Advanced**] を選択します。
   その他のプロパティが表示されます。
4. [**Authentication Profiles**] リストの [**Available**] ボックスで、先に作成したカスタム TACACS+ プロファイルの名前を選択し、Move ボタン（<<）をクリックします。
   選択したプロファイル名が [**Enabled**] ボックスに移動します。

   注 : [Authentication Profiles] *リストを変更できない場合は、現在のユーザロールではバーチャルサーバを変更する権限が与えられていないことを示します。*
5. [**Update**] をクリックします。

リモート LDAP サーバを使用した SSL ベースの承認の設定

SSL クライアント証明書 LDAP 認証モジュールを使用することにより、リモート LDAP サーバでアプリケーショントラフィックのアクセス制御を実行することができます。このモジュールは、SSL 証明書とユーザ指定のロールに基づいてアクセス制御を行います。

アプリケーショントラフィックに対して SSL Client Certificate LDAP に基づく認証を設定するには、次の作業を完了します。

- SSL クライアント証明書 LDAP タイプの構成オブジェクトを作成する
- SSL クライアント証明書 LDAP タイプの認証プロファイルを作成する
- HTTPトラフィックの管理用に構成されたバーチャルサーバを変更する

SSL クライアント証明書 LDAP 構成オブジェクトの作成

BIG-IP で SSL クライアント証明書 LDAP ベースのリモート認証を設定するには、最初に、設定ユーティリティを使用してカスタム SSL クライアント証明書 LDAP 構成オブジェクトを作成してください。***SSL クライアント証明書 LDAP 構成オブジェクト***では、BIG-IP がリモート認証を実行するために必要な情報を指定します。

カスタム SSL クライアント証明書 LDAP 構成オブジェクトを作成したら、カスタム SSL クライアント証明書 LDAP プロファイルを作成し、このカスタムプロファイルを SSL バーチャルサーバに割り当てます。

カスタム SSL クライアント証明書 LDAP 構成オブジェクトの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. [Authentication] メニューの [Configurations] を選択します。
   [Authentication Configurations] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
   [New Authentication Configuration] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールでは SSL Client Certificate LDAP 構成オブジェクトを作成する権限が与えられていないことを示します。*
4. [**Name**] ボックスに、構成オブジェクトに一意の名前（**my_ssl_client_cert_ldap_config** など）を入力します。
5. [**Type**]リストから、[**SSL Client Certificate LDAP**] を選択します。
   これで、ユーザ設定可能な構成オブジェクト設定が表示されます。

6. [Configuration] 領域では、[**Basic**] または [**Advanced**] を選択します。
[**Advanced**] を選択した場合、追加の設定項目が画面に表示されます。
7. [**Hosts**] 設定で、次の作業を行います。
a) リモート LDAP の IP アドレスを入力します。
b) [**Add**] をクリックします。
IP アドレスがテキストウィンドウに表示されます。
8. [**Search Type**] リストから、[**User**]、[**Certificate Map**]、または [**Certificate**] を選択します。
9. [**User Base DN**] ボックスに、LDAP サーバが [**User**] 検索タイプまたは[**Certificate**]検索タイプの実行に使用するサブツリーの検索ベースを入力します。
10. [**User Key**] ボックスに、LDAP がユーザ ID の指定に使用する属性を入力します。
11. 手順 6 で基本的な構成を選択した場合は、[**Finished**] をクリックします。手順 6 で詳細な構成を選択した場合は、残りの設定を継続し、[**Finished**] をクリックします。

SSL クライアント証明書 LDAP 認証プロファイルの作成

BIG-IP で LDAP ベースのリモート認証を設定する次の作業は、カスタム SSL クライアント証明書 LDAP プロファイルの作成です。***SSL クライアント証明書 LDAP 認証プロファイル***では、先に作成した LDAP 構成オブジェクトの名前などの情報を指定します。

カスタム SSL クライアント証明書 LDAP プロファイルを作成したら、このカスタムプロファイルとデフォルトの iRule をバーチャルサーバに割り当てます。

カスタム SSL クライアント証明書 LDAP プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
[HTTP Profiles] 画面が開きます。
2. [Authentication] メニューの [Profiles] を選択します。
[Authentication Profiles] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
[New Authentication Profile] 画面が開きます。
注 : [Create] ボタンをクリックできない場合は、現在のユーザロールでは SSL Client Certificate LDAP プロファイルを作成する権限が与えられていないことを示します。
4. [**Name**] ボックスに、プロファイルに一意の名前（**my_ssl_client_cert_ldap_profile** など）を入力します。

5. [**Type**]リストから、[**SSL Client Certificate LDAP**]を選択します。
これで、ユーザ設定可能なプロファイル設定が表示されます。
6. [**Parent Profile**] リストで [**sol ldap**] が選択されていることを確認します。
これで、**ldap** という名前のデフォルトプロファイルからデフォルトの構成値が新しいプロファイルに継承されます。
7. [**Configuration**] リストから、先に作成した LDAP 構成オブジェクトの名前を選択します。
8. 残りの設定はすべて、デフォルト値をそのまま使用します。
9. [**Finished**] をクリックします。

SSL クライアント証明書 LDAP 承認用バーチャルサーバの変更

リモート LDAP サーバによる承認の実装プロセスでの最後の作業は、カスタム SSL クライアント証明書 LDAP プロファイルとデフォルトの LDAP 認証 iRule を、HTTP トラフィック処理用に構成されたバーチャルサーバ（すなわち、HTTP プロファイルが割り当てられたバーチャルサーバ）に割り当てる作業です。

◆注

プロファイルと iRule を割り当てるバーチャルサーバは、標準タイプのバーチャルサーバでなければなりません。

バーチャルサーバを SSL クライアント証明書 LDAP 承認用に変更する方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
[Virtual Servers] 画面が開きます。
2. Name カラムで、HTTP サーバプロファイルを割り当てる標準タイプバーチャルサーバの名前をクリックします。
選択したバーチャルサーバのプロパティが表示されます。
3. [**Configuration**] リストから、[**Advanced**] を選択します。
その他のプロパティが表示されます。
4. [**Authentication Profiles**] リストの [**Available**] ボックスで、先に作成したカスタム SSL クライアント証明書 LDAP プロファイルの名前を選択し、Move ボタン（<<）をクリックします。
選択したプロファイル名が [**Enabled**] ボックスに移動します。

   注 : [Authentication Profiles] *リストを変更できない場合は、現在のユーザロールではバーチャルサーバを変更する権限が与えられていないことを示します。*
5. [**Update**] をクリックします。

OCSP レスポンダを使用した SSL 証明書失効の設定

SSL OCSP 認証モジュールとは、ローカルトラフィック管理システム経由のクライアント接続を認証するための機構です。さらに具体的に言うと、***SSL OCSP 認証モジュール*** は、SSL 証明書の失効状態をその証明書の認証の一部としてチェックします。

OCSP認証モジュールを実装するには、次の作業を行う 必要があります。

- 1 つ以上の上位 OCSP レスポンダオブジェクトを作成する
- SSL OCSP 構成オブジェクトを作成する
- SSL OCSP プロファイルを作成する
- バーチャルサーバを変更し、SSL OCSP プロファイルをそのバーチャルサーバへ割り当てる

SSL OCSP レスポンダオブジェクトの作成

BIG-IP で SSL OCSP ベースのリモート認証を設定するには、最初に、カスタム SSL OCSP レスポンダオブジェクトを作成してください。***SSL OCSP レスポンダオブジェクト***とは、外部 SSL OCSP レスポンダの URL を含めるように作成するオブジェクトです。外部 SSL OCSP レスポンダごとに別個のSSL OCSPレスポンダオブジェクトを作成する必要があります。

カスタム SSL OCSP レスポンダオブジェクトを作成したら、カスタム SSL OCSP 構成オブジェクトとカスタム SSL OCSP プロファイルを作成し、このカスタムプロファイルとデフォルトの iRule を HTTP バーチャルサーバに割り当てます。

SSL OCSP レスポンダオブジェクトの作成方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Profiles**] をクリックします。
   [Profiles] 画面が開きます。
2. [Authentication] メニューの [OCSP Responders] を選択します。
   [OCSP Responders List] 画面が表示されます。
3. 画面の右上で [**Create**] をクリックします。
   [New OCSP Responder] 画面が表示されます。

   注 : [Create] *ボタンをクリックできない場合は、現在のユーザロールではSSL OCSP レスポンダオブジェクトを作成する権限が与えられていないことを示します。*
4. [**Name**] 設定に、OCSP レスポンダオブジェクトに一意の名前（**my_ocsp_responder** など）を入力します。
5. 値を入力するか引き継ぐことにより、すべての設定項目に値を指定します。
6. [**Finished**] をクリックします。

SSL OCSP 構成オブジェクトの作成

BIG-IP で SSL OCSP ベースのリモート認証を設定する次の作業は、カスタム SSL OCSP 構成オブジェクトの作成です。***SSL OCSP 構成オブジェクト***では、BIG-IP がリモート認証を実行するために必要な情報を指定します。

カスタム SSL OCSP 構成オブジェクトの作成したら、カスタム SSL OCSP プロファイルを作成し、このカスタムプロファイルを HTTP バーチャルサーバに割り当てます。

SSL OCSP 構成オブジェクトの作成方法

1. [Main] タブで [**Local Traffic**] を展開し、[**Profiles**] をクリックします。
   [Profiles] 画面が開きます。
2. [**Authentication**] メニューの [**Configurations**] を選択します。
   [Authentication Configurations] 画面が表示されます。
3. 画面の右上で [**Create**] をクリックします。
   [New Authentication Configuration] 画面が表示されます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではSSL OCSP構成オブジェクトを作成する権限が与えられていないことを示します。
4. [**Name**] 設定に、構成オブジェクトに一意の名前（**my_ocsp_config** など）を入力します。
5. [**Type**] 設定から [**SSL OCSP**] を選択します。
6. [**Responders**] 設定の [**Available**] ボックスから、OCSP レスポンダオブジェクトの名前を選択し、Move ボタン（<<）をクリックします。
   選択した名前が [**Selected**] ボックスに移動します。
7. 各レスポンダオブジェクトに対して上記手順を繰り返します。
8. [**Finished**] をクリックします。

SSL OCSP プロファイルの作成

BIG-IP で SSL OCSP ベースのリモート認証を設定する次の作業は、カスタム SSL OCSP プロファイルの作成です。***SSL OCSP プロファイル***では、先に作成した SSL OCSP 構成オブジェクトの名前などの情報を指定します。

プロファイルを作成したら、このカスタムプロファイルとデフォルトの iRule をバーチャルサーバに割り当てます。

カスタム SSL OCSP プロファイルの作成方法

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。

2. [Authentication] メニューの [Profiles] を選択します。
[Authentication Profiles] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
[New Authentication Profile] 画面が開きます。

   注 : [Create] ボタンをクリックできない場合は、現在のユーザロールではSSL OCSP プロファイルを作成する権限が与えられていないことを示します。
4. [**Type**] リストから、[**SSL OCSP**] を選択します。
これで、ユーザ設定可能なプロファイル設定が表示されます。
5. [**Name**] ボックスに、プロファイルに一意の名前（**my_ssl_ocsp_profile** など）を入力します。
6. [**Parent Profile**] リストで [**ssl_ocsp**] が選択されていることを確認します。
これで、**ssl_ocsp** という名前のデフォルトプロファイルからデフォルトの構成値が新しいプロファイルに継承されます。
7. [**Configuration**] リストから、先に作成した SSL OCSP 構成オブジェクトの名前を選択します。
8. 残りの設定はすべて、デフォルト値をそのまま使用します。
9. [**Finished**] をクリックします。

SSL OCSP 認証用バーチャルサーバの変更

リモート SSL OCSP 認証の実装プロセスでの最後の作業は、カスタム SSL OCSP プロファイルを、HTTP トラフィック処理用に構成されたバーチャルサーバ（すなわち、HTTP プロファイルが割り当てられたバーチャルサーバ）に割り当てる作業です。

◆注

認証プロファイルを割り当てるバーチャルサーバは、標準タイプのバーチャルサーバでなければなりません。

SSL OCSP 認証用バーチャルサーバの変更方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Virtual Servers**] をクリックします。
[Virtual Servers] 画面が開きます。
2. [Name] カラムで、バーチャルサーバの名前をクリックします。
選択したバーチャルサーバのプロパティが表示されます。
3. [**Configuration**] リストから、[**Advanced**] を選択します。
その他のプロパティが表示されます。
4. [**Authentication Profiles**] リストの [**Available**] ボックスで、先に作成したカスタム SSL OCSP プロファイルの名前を選択し、**Move** ボタン（<<）をクリックします。
選択したプロファイル名が [**Enabled**] ボックスに移動します。

*注 : [**Authentication Profiles**] リストを変更できない場合は、現在のユーザロールではバーチャルサーバを変更する権限が与えられていないことを示します。*

5. [**Update**] をクリックします。

CRLDP 認証モジュールの設定

Certificate Revocation List Distribution Point（CRLDP）認証モジュールとは、ローカルトラフィック管理システム経由のクライアント接続を認証するための機構です。さらに具体的に言うと、***CRLDP 認証モジュール***は、SSL 証明書の失効状態をその証明書の認証の一部としてチェックします。

CRLDP 認証モジュールを実装するには、次の作業を行う必要があります。

- 1 つ以上の上位 CRLDP サーバオブジェクトを作成する
- CRLDP 構成オブジェクトを作成する
- CRLDP プロファイルを作成する
- バーチャルサーバを変更し、CRLDP プロファイルをそのバーチャルサーバへ割り当てる

CRLDP サーバオブジェクトの作成

BIG-IP で CRLDP ベースのリモート認証を設定するには、最初に、カスタム CRLDP サーバオブジェクトを作成してください。***CRLDP サーバオブジェクト***とは、外部 CRLDP サーバの URL を含めるように作成されるオブジェクトです。外部 CRLDP サーバごとに別個の CRLDP レスポンダオブジェクトを作成する必要があります。

カスタム CRLDP オブジェクトを作成したら、カスタム CRLDP 構成オブジェクトとカスタム CRLDP プロファイルを作成し、このカスタムプロファイルとデフォルトの iRule を HTTP バーチャルサーバに割り当てます。

CRLDP レスポンダオブジェクトを作成するには

1. [Main] タブの [**Local Traffic**] を展開します。
2. [**Profiles**] をクリックします。
   [Profiles] 画面が開きます。
3. [Authentication] メニューの [CRLDP Servers] を選択します。
   [CRLDP Servers list] 画面が表示されます。
4. 画面の右上で [**Create**] をクリックします。
   [New CRLDP Server] 画面が表示されます。

   *注 : [**Create**] ボタンをクリックできない場合は、現在のユーザロールではCRLDP レスポンダオブジェクトを作成する権限が与えられていないことを示します。*

5. **my_crldp_server** など、CRLDP サーバオブジェクトの一意の名前を **[Name]** 設定に入力します。
6. 値を入力するか引き継ぐことにより、すべての設定項目に値を指定します。
7. **[Finished]** をクリックします。

CRLDP 構成オブジェクトの作成

BIG-IP で CRLDP ベースのリモート認証を設定するには、カスタム CRLDP 構成オブジェクトを作成してください。***CRLDP 構成オブジェクト***では、BIG-IP がリモート認証を実行するために必要な情報を指定します。

カスタム CRLDP 構成オブジェクトを作成したら、カスタム CRLDP プロファイルを作成し、このカスタムプロファイルを HTTP バーチャルサーバに割り当てます。

CRLDP 構成オブジェクトを作成するには

1. [Main] タブで **[Local Traffic]** を展開し、**[Profiles]** をクリックします。
   [Profiles] 画面が開きます。
2. **[Authentication]** メニューの **[Configurations]** を選択します。
   [Authentication Configurations] 画面が表示されます。
3. 画面の右上で **[Create]** をクリックします。
   [New Authentication Configuration] 画面が表示されます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではCRLDP 構成オブジェクトを作成する権限が与えられていないことを示します。*
4. **[Name]** 設定に、構成オブジェクトに一意の名前（**my_crldp_config** など）を入力します。
5. **[Type]** 設定から **[CRLDP]** を選択します。
6. **[Servers]** 設定の **[Available]** ボックスから、CRLDP サーバオブジェクトの名前を選択し、Move ボタン（**<<**）をクリックします。選択した名前が **[Selected]** ボックスに移動します。
7. 各サーバオブジェクトに対して上記手順を繰り返します。
8. **[Finished]** をクリックします。

CRLDP プロファイルの作成

BIG-IP で CRLDP ベースのリモート認証を設定するには、カスタム CRLDP プロファイルを作成してください。***CRLDP プロファイル***では、先に作成した CRLDP 構成オブジェクトの名前などの情報を指定します。

プロファイルを作成したら、このカスタムプロファイルとデフォルトの iRule をバーチャルサーバに割り当てます。

カスタム CRLDP プロファイルを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [HTTP Profiles] 画面が開きます。
2. [Authentication] メニューの [Profiles] を選択します。
   [Authentication Profiles] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
   [New Authentication Profile] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではCRLDP プロファイルを作成する権限が与えられていないことを示します。*
4. [**Type**] リストから、[**CRLDP**] を選択します。
   これで、ユーザ設定可能なプロファイル設定が表示されます。
5. [**Name**] ボックスに、プロファイルに一意の名前（**my_crldp_profile** など）を入力します。
6. [**Parent Profile**] リストで [**ssl_crldp**] が選択されていることを確認します。
   これで、**ssl_crldp** という名前のデフォルトプロファイルからデフォルトの構成値が新しいプロファイルに継承されます。
7. [**Configuration**] リストから、先に作成した CRLDP 構成オブジェクトの名前を選択します。
8. 残りの設定はすべて、デフォルト値をそのまま使用します。
9. [**Finished**] をクリックします。

CRLDP 認証用バーチャルサーバの変更

リモート CRLDP 認証の実装プロセスでの最後の作業は、カスタム CRLDP プロファイルを、HTTP トラフィック処理用に構成されたバーチャルサーバ（すなわち、HTTP プロファイルが割り当てられたバーチャルサーバ）に割り当てる作業です。

◆注

認証プロファイルを割り当てるバーチャルサーバは、標準タイプのバーチャルサーバでなければなりません。

CRLDP 認証用バーチャルサーバの変更方法

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. [Name] カラムで、バーチャルサーバの名前をクリックします。
   選択したバーチャルサーバのプロパティが表示されます。
3. [**Configuration**] リストから、[**Advanced**] を選択します。
   その他のプロパティが表示されます。

4. [**Authentication Profiles**] リストの [**Available**] ボックスで、先に作成したカスタム CRLDP プロファイルの名前を選択し、**Move** ボタン（<<）をクリックします。
選択したプロファイル名が [**Enabled**] ボックスに移動します。

   注 : [Authentication Profiles] *リストを変更できない場合は、現在のユーザロールではバーチャルサーバを変更する権限が与えられていないことを示します。*

5. [**Update**] をクリックします。

26

Kerberos 委任の設定

- Kerberos 委任インフラストラクチャの概要
- BIG-IP での Kerberos 委任の設定
- Kerberos 委任設定の作成
- クライアントトラフィックの認証

Kerberos 委任インフラストラクチャの概要

Kerberos 委任は、Microsoft Windows Integrated Authentication を使用してクライアントトラフィックを認証する機能を提供します。2 つの領域が信頼関係を持つ場合には、クロス領域認証を設定することもできます。

表 26.1 は、Kerberos 委任のインフラストラクチャ要件を示します。

インフラストラクチャ	構成要件
プライマリドメイン コントローラ	この Kerberos 委任のシナリオでは、Microsoft® プライマリドメインコントローラ（PDC）を使用します。 PDC 上の時間は、クライアントおよび Web サーバ上の時間と同期していることが必要です。 プライマリドメインコントローラは、DNS サーバであり、各種 Web サーバを認識している必要があります。
クライアント	クライアントマシンは、ドメイン内になければなりません。 クライアント上の時刻は、Web サーバおよび PDC 上の時刻と同期していることが必要です。 クライアントは、Windows Internet Explorer バージョン 3.x 以降を使用する必要があります。
Web サーバ	Web サーバは、匿名アクセスを禁止して Windows® Integrated Authentication を使用するようにセットアップされている必要があります。サーバプールに複数のサーバをセットアップする予定がある場合には、Kerberos Web サーバの負荷分散に関する詳細について、Microsoft のドキュメントを参照してください。 Web サーバ上の時刻は、クライアントおよび PDC 上の時刻と同期していることが必要です。
BIG-IP	BIG-IP は、PDC を含むドメインに配置されていることが必要です。 BIG-IP は、クライアントとその Web サーバの間のセキュアなトラフィックを処理できる必要があります。 BIG-IP は、PDC を認識している DNS サーバを使用する必要があります。 BIG-IP 上の時刻は、PDC と同期していることが必要です。

***表 26.1** Kerberos 委任のインフラストラクチャ要件*

BIG-IP での Kerberos 委任の設定

BIG-IP に Kerberos 委任を設定するには、以下のタスクを終了する必要があります。

- BIG-IP への DNS サーバの追加
- 信頼済みドメインへの BIG-IP の参加
- Kerberos 委任設定のセットアップ

BIG-IP への DNS サーバの追加

BIG-IP に Kerberos 委任を設定するための最初の手順は、BIG-IP への DNS サーバの追加です。このセクションでは、BIG-IP から DNS サーバをテストする方法を説明するとともに、設定ユーティリティまたはコマンドラインインターフェイスから DNS サーバを BIG-IP に追加する方法について説明します。

BIG-IP で DNS サーバを定義する前に DNS サーバをテストするには

BIG-IP で DNS サーバを設定する前に、BIG-IP で定義する予定の DNS サーバをテストするには、Linux プロンプトで以下のコマンドを入力します。

```
dig @<DNS_Server_IP_Address>
```

テストが成功した場合、ルートネームサーバの一覧が表示されます。

設定ユーティリティを使用して DNS 名前解決を設定するには

1. ナビゲーションペインの [Main] タブで、[**System**] を展開して [**Configuration**] をクリックします。
   [General] 画面が開きます。
2. [Device] メニューから [DNS] を選択します。
   [DNS] 画面が開きます。
3. **DNS Lookup Server List** 設定を探します。
4. [**Address**]ボックスに、DNSサーバのIPアドレスを入力します。
5. [**Add**] をクリックします。
6. [**Update**] をクリックします。

コマンドラインから DNS 名前解決を設定するには

1. コマンドラインにログインします。
2. 以下のコマンドを入力して、BIG-IP 上に DNS サーバを定義します。

   ```
   bigpipe dns nameservers <DNS_Server_IP_Address> add
   ```

たとえば、DNS ネームサーバ IP アドレス **192.168.10.20** および **192.168.10.22** を BIG-IP に追加する場合には、以下のコマンドを入力します。

```
bigpipe dns nameservers 192.168.10.20 192.168.10.22 add
```

3. 以下のコマンドを入力して、変更を保存します。

```
bigpipe save
```

ローカルの **/etc/resolv.conf** ファイルは、現在、以下のエントリで構成されています。

```
nameserver      192.168.10.20
nameserver      192.168.10.22
```

信頼済みドメインへの BIG-IP の参加

DNS サーバを BIG-IP に追加した後、BIG-IP を信頼済みドメインに追加することができます。BIG-IP を信頼済みドメインに追加するには、**domaintool** コマンドを使用します。

BIG-IP をこのドメインに追加するために **domaintool** コマンドを使用しますが、ここで、**<domainname>** は、すべて大文字のドメイン名です。また、**<name>** は、Kerberos Key Distribution Center（KDC）の FQDN です。オプションで、KDC の IP アドレスを使用できます。コマンド構文は次のとおりです。

```
domaintool --add <domainname> --kdc <name|IP address>
```

クロスドメイン認証をセットアップする場合は、**--dnsdomain** オプションをこのコマンドに使用します。特定の DNS ドメインで検出されたすべてのホストは、自動的に正しい Kerberos 領域に配置されます。BIG-IP が通信する可能性のある領域ごとに、**domaintool --add** コマンドを使用してください。

BIG-IP において通信する可能性のあるドメインが設定されましたので、**domaintool** コマンドを使用して、ドメイン内にサービスプリンシパルを作成する必要があります。これらのサービスプリンシパルは、作成するバーチャルサーバの FQDN を使用して名前が付けられます。

```
domaintool --join <domainname> --admin_principal <admin principal> --host <hostname>
```

このコマンドでは、パスワードが要求されます。通常、**admin_principal** 引数の値は **administrator** ですが、任意の管理者名を使うことができます。**host** 引数は、トラフィック用に設定するバーチャルサーバの FQDN を指定します。設定する予定のバーチャルサーバごとにこのコマンドを実行します。

◆ 重要

*これらのコマンドの詳細については、**domaintool** のマニュアルページを参照してください。*

Kerberos 委任設定の作成

DNS サーバを BIG-IP に追加し、BIG-IP をドメインに追加した後は、Kerberos 委任設定を作成する必要があります。このセクションでは、Kerberos 委任設定を設定ユーティリティから作成する方法（後述）とコマンドラインインターフェイスから作成する方法（「*コマンドラインからの Kerberos 委任の設定*」（26-7 ページ））を示します。

この設定を作成するには、以下のオブジェクトを作成する必要があります。

- Kerberos 委任設定
- Kerberos 委任プロファイル
- Kerberos 委任 Client SSL プロファイル
- 負荷分散用の Kerberos 委任プール
- Kerberos 委任バーチャルサーバ

◆ 重要

*Kerberos 委任プロファイルには、**set-cookie** 操作が含まれます。確実に攻撃者がこの **set-cookie** ヘッダをインターセプトできないようにするには、常に Client SSL プロファイルと組み合わせて Kerberos 委任プロファイルを使用してください。*

設定ユーティリティを使用した Kerberos 委任の設定

このセクションでは、設定ユーティリティを使用した Kerberos 委任の設定手順のすべてを提供します。コマンドラインインターフェイスを使用した Kerberos 委任の設定手順は、「*コマンドラインからの Kerberos 委任の設定*」（26-7 ページ）で説明します。

Kerberos 委任設定オブジェクトを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [**Profiles**] 画面が開きます。
2. [Authentication] メニューの [Configurations] を選択します。
   [Authentication Configurations] 画面が開きます。
3. 画面右上の [**Create**] をクリックします。
   [New Authentication Configuration] 画面が開きます。
4. [**Name**] 設定に、設定オブジェクトの固有の名前（**my_kerberos_config** など）を入力します。

   注：名前のアルファベット文字はすべて小文字でなければなりません。
5. [**Type**] 設定から [**Kerberos Delegation**] を選択します。
   画面が拡張され、いくつかの設定が表示されます。

6. [**Client Principal Name**] ボックスに、クライアントプリンシパル名を入力します。
クライアントプリンシパル名は、BIG-IP 上のバーチャルサーバの名前です。以下のフォーマットを使用します。ここで、**<name>** は、先の手順でドメインに追加した **admin_principal** 名です。
HTTP/<name>
7. [**Server Principal Name**] ボックスに、サーバプリンシパル名を入力します。
サーバプリンシパル名は、Web サーバの名前です。以下のフォーマットを使用します。ここで、**<FQDN>** は、プール内の Web サーバの完全修飾ドメイン名です。
HTTP/<FQDN>
8. [**Finished**] をクリックします。

Kerberos 委任プロファイルオブジェクトを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
[Profiles] 画面が開きます。
2. [Authentication] メニューの [Profiles] を選択します。
[Authentication Profiles] 画面が開きます。
3. 画面の右上で [**Create**] をクリックします。
[New Authentication Profile] 画面が開きます。
4. **my_kerberos_profile** など、構成オブジェクトの一意の名前を [**Name**] 設定に入力します。
注：名前のアルファベット文字はすべて小文字でなければなりません。
5. [**Type**] 設定から [**Kerberos Delegation**] を選択します。
画面が拡張され、いくつかの設定が表示されます。
6. [**Cookie Name**] 設定に、固有の名前を入力します。
7. [**Cookie Key**] 設定に、文字列パスワードを入力します。
*注：**Cookie Key** の値は、Cookie データを暗号化する暗号鍵です。デフォルト値は提供されていますが、この値を知っている攻撃者が Cookie データを復号し、信頼済みのユーザを偽装することがないようにするため、このデフォルト値は変更してください。*
8. [**Finished**] をクリックします。

Client SSL プロファイルを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
プロファイルのリストが表示されます。
2. [**SSL**] メニューから、[Client] を選択します。
既存の SSL プロファイルのリストが表示されます。

3. 画面右上の [**Create**] をクリックします。
   [New Client SSL Profiles] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*

4. [**Name**] ボックスに、プロファイルの一意の名前を入力します。
5. 画面右端の [**Custom**] ボックスをクリックします。
6. [**証明書**] リストから、既存の証明書の名前を選択します。
7. [**Key**] リストから、既存の鍵の名前を選択します。
8. 画面下部の [**Finished**] をクリックします。

ロードバランシングプールを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   [Pools] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Pool] 画面が開きます。

   ***注 : [Create]** ボタンをクリックできない場合は、現在のユーザロールではプールを作成する権限が与えられていないことを示します。*

3. [**Configuration**] リストから、[**Advanced**] を選択します。
4. [**Name**] 設定で、プールの名前（**webserverpool** など）を入力します。
5. その他の設定を指定します。そのまま使用することや変更することもできます。

   ***注 : [New Members]** 設定には、Kerberos 委任インフラストラクチャ内の各 Web サーバの IP アドレスとポートを追加してください。*

6. [**Finished**] をクリックします。

バーチャルサーバを作成し、Kerberos 委任と Client SSL プロファイルをバーチャルサーバに追加するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Servers] 画面が開きます。
2. 画面右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。
3. [**Name**] 設定に、バーチャルサーバの固有の名前（**my_kerberos_virtual** など）を入力します。
4. [**Destination**] 設定で [**Host**] をクリックし、IP アドレスを入力します。
5. [**Service Port**] 設定に **80** と入力するか、サービスのリストから [**HTTP**] を選択します。

6. [**Configuration**] リストから、[**Advanced**] を選択します。
7. [**Type**] 設定から [**Standard**] を選択します。
8. [**Protocol**] 設定で [**TCP**] を選択します。
9. [**HTTP Profile**] 設定で [**http**] を選択します。
10. [**SSL Profile (Client)**] リストから、先に作成した Client SSL の名前を選択します。
11. [**Authentication Profiles**] 設定で、**移動**ボタン（[<<] または [>>]）を使用して、Kerberos 委任用に作成したプロファイルを有効にします。
12. 画面の [Resources] 領域で、[**Default Pool**] リストから、先に作成した、Web サーバを含むプールを選択します。
13. [**Finished**] をクリックします。

コマンドラインからの Kerberos 委任の設定

このセクションでは、**bigpipe** ユーティリティを使用して、コマンドランからKerberos委任を作成する方法を説明します。設定ユーティリティを使用した Kerberos 委任の設定については、「*設定ユーティリティを使用した Kerberos 委任の設定*」（26-4 ページ）をご覧ください。

コマンドラインから Kerberos 委任設定オブジェクトを作成するには

Kerberos 委任設定オブジェクトを作成するには、以下のコマンドを入力します。

```
auth krbdelegate my_kerberos_config { server principal "HTTP/<FQDN>" client principal
    "HTTP/<FQDN>" }
```

サーバプリンシパルに対しては、Web サーバの完全修飾ドメイン名（FQDN）を使用します。

各クライアントプリンシパルに対しては、BIG-IP 上に作成する予定のバーチャルサーバの FQDN を使用します。

コマンドラインから Kerberos 委任プロファイルオブジェクトを作成するには

Kerberos 委任設定オブジェクトを作成した後、設定のプロファイルの作成ができます。

必ず Cookie 名と Cookie 暗号鍵の文字列パスワードのセットをプロファイルに設定してください。この例では、Cookie 名が **kerbc**、鍵が **kerbc** です。

```
profile auth my_kerberos_profile { defaults from krbdelegate config my_kerberos_config
    type krbdelegate cookie name kerbc cookie key "kerbc" }
```

◆注

***Cookie Key** の値は、Cookie データを暗号化する暗号鍵です。デフォルト値は提供されていますが、この値を知っている攻撃者がCookie データを復号し、信頼済みのユーザを偽装することがないようにするため、このデフォルト値は変更してください。*

コマンドラインから Client SSL を作成するには

Kerberos 委任設定の次のタスクは、Client SSL プロファイルの作成です。**profile clientssl** コマンドを以下のように入力します。

```
profile clientssl my_client_ssl_profile ( defaults from clientssl key my_key_name cert
    my_cert_name )
```

コマンドラインからロード バランシングプールを作成するには

Kerberos 委任設定の設定オブジェクトとプロファイルを作成した後、コマンドラインを使用して、Web サーバのプールを作成します。ここで、**<ip addr>** は、Web サーバの IP アドレスです。

```
pool webserverpool { monitor all http members <ip addr>:http }
```

コマンドラインから Kerberos 委任バーチャルサーバを作成するには

BIG-IP に Kerberos 委任を設定するための最後の手順は、委任用のバーチャルサーバの作成です。

バーチャルサーバを作成するには、以下のコマンドを入力します。ここで、**<ip addr>:http** はバーチャルサーバのアドレス、**webserverpool** は Web サーバのプール、**my_client_profile** は、作成した Client SSL プロファイル、**my_kerberos_profile** は、Kerberos 委任用に作成したプロファイルです。

```
virtual my_kerberos_virtual { snat automap pool webserverpool destination <ip addr>:http
    ip protocol tcp profiles http tcp my_clientssl_profile auth my_kerberos_profile }
```

クライアントトラフィックの認証

ネットワークの設定が終了し、BIG-IP の設定が終了すると、Kerberos 委任によりクライアントが認証されます。図 26.1 は、Kerberos 委任によるクライアント認証の動作を示します。

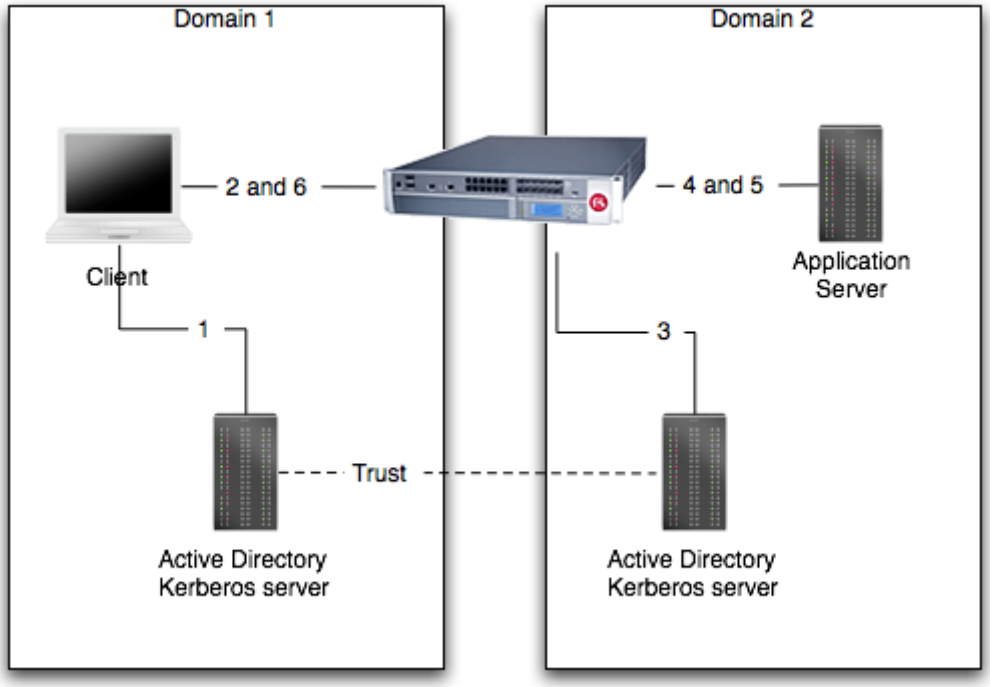

***図 26.1** Kerberos 委任によるクライアントトラフィックの認証動作*

Kerberos 委任によるクライアントトラフィックの認証プロセスは、以下のようになります。

1. ユーザがドメインにログインします。
2. クライアントブラウザは、BIG-IP バーチャルサーバに接続し、Windows Integrated Authentication 認証情報と SSL 認証情報を渡します。
3. BIG-IP は、認証情報を検証し、これらの認証情報を使用して、ドメイン 1 のユーザに代わってドメイン 2 の認証情報を取得します。
4. BIG-IP は、手順 3 で取得した認証情報を、ドメイン 2 のアプリケーションサーバに渡します。
5. アプリケーションが応答します。
6. BIG-IP は、応答をクライアントに渡します。

27

複数の認証サーバの設定

- 複数の認証サーバ設定の概要
- 前提条件
- BIG-IP システムオブジェクトの設定

複数の認証サーバ設定の概要

BIG-IP の特徴の 1 つは、リモートの LDAP、RADIUS、または TACACS+ サーバにユーザアカウントを保存する場合のローカル管理トラフィックを認証する機能です。実際には、1 台のみではなく、2 台のリモートサーバをローカル管理トラフィックの認証用に BIG-IP で設定することができます。大半のカスタマには、1 台または 2 台のリモート認証サーバを設定できる機能で十分すぎるほどです。しかし、潜在的に次の 2 つの問題があります。

- カスタマによっては、ローカル認証用に 2 台以上のリモートサーバを必要とする。
- 認証の際、1 台またはそれ以上のサーバが利用できない場合であっても、BIG-IP は特定の順序（サーバ 1、サーバ 2 の順）でサーバにクエリする。このため、すべての着信接続で TCP タイムアウトが発生し、パフォーマンスの低下を引き起こす可能性があります。

これらの問題は、仮想認証サーバを作成して解決できます。***仮想認証サーバ*** は、付加的なリモート LDAP、RADIUS、または TACACS+ サーバとして動作するバーチャルサーバです。必要な台数の仮想認証サーバを設定することができます。

通常、複数の仮想認証サーバを実装するには、以下の作業を行う必要があります。

- まず、ヘルスモニタを作成してサーバノードのモニタを行い、それらサーバノードの **up** または **down** の状態を検知します。
- 次に、サーバオブジェクト（RADIUS サーバの場合のみ）と認証構成オブジェクトを作成します。
- 次に、ロードバランシングプールを作成し、複数の認証サーバをこのプールのメンバに設定して、先に作成したモニタでこれらのサーバをモニタします。down とマークされたサーバノードに対しては、BIG-IP による認証の際のクエリは行われません。
- 最後に、仮想認証サーバを作成し、これをサーバのプールに関連付けます。さらに、アプリケーションのターゲットをこのバーチャルサーバに設定します。

◆注

プールをバーチャルサーバに関連付ける代わりに、各プロキシまたは認証ソースをプールに直接関連付けることもできます。

ここからは、複数の認証サーバ構成を正しく作成する方法について説明します。例として、RADIUS サーバの場合について記載していますが、LDAP や TACACS+ サーバの場合にも、わずかな相違点はありますが、同様に適用できます。具体的には、LDAP または TACACS+ サーバの場合は、RADIUS secret に関する情報は不要となります。また、RADIUS 構成オブジェクトの記述は、LDAP または TACACS+ 構成オブジェクトに置き換えてお読みください。RADIUS サーバオブジェクトに関する情報は無視してもかまいません。

前提条件

作業を始める前に、次の条件を満たしていることを確認してください。

- RADIUS secret は、すべての RADIUS サーバで同一であること。
- RADIUS プールを参照するために作成するバーチャルサーバのアドレスは、ループバックアドレスではないこと。
- RADIUS プールを参照するバーチャルサーバは、各種 RADIUS サーバと同一の VLAN にあること。
  たとえば、RADIUS サーバのアドレスが **10.1.1.10** と **10.1.1.11** で、これらが VLAN **internal** にある場合、これらのアドレスに転送可能なバーチャルサーバ（**10.1.1.99** など）に RADIUS プールを関連付ける必要があります。このため、RADIUS トラフィックの送信元アドレスは、バーチャルサーバアドレスではなく、VLAN **internal** のセルフ IP アドレスとなります。

BIG-IP システムオブジェクトの設定

複数の RADIUS サーバ構成を作成するには、ローカルトラフィックオブジェクトの設定が必要です。表 27.1 は、これらのオブジェクトと、これらのオブジェクトの作成に使用する設定ユーティリティの画面を示します。これらの画面はすべて、[Main] タブの [**Local Traffic**] にある設定ユーティリティからアクセスできます。これらの画面の詳細については、オンラインヘルプを参照してください。

オブジェクト	設定ユーティリティ画面
RADIUS ヘルスモニタ	Monitors
RADIUS サーバオブジェクト	Profiles
RADIUS サーバオブジェクトを参照する RADIUS 構成オブジェクト	Profiles
RADIUSヘルスモニタを参照するロードバランシングプール	Pools
ロードバランシングプールを参照するバーチャルサーバ	Virtual Servers

***表 27.1** 必要な設定ユーティリティの画面*

図 27.1 に、**bigip.conf** ファイルの関連エントリの例を示します。

```
monitor my_radius_monitor {
    defaults from radius
    password "jdoe"
    secret "testing123"
    username "jdoe"
}
radius server system_auth_name1 {
    host "10.1.1.99"
    service 1645
    secret "testing123"
}
auth radius system-auth {
    server system_auth_name1
}
pool radius_pool {
    monitor all my_radius_monitor
    member 10.1.1.10:1812
    member 10.1.1.12:1645
}
virtual radius_virtual_server {
    destination 10.1.1.99:1645
    ip protocol udp
    pool radius_pool
```

***図 27.1** bigip.conf ファイルの関連エントリの例*

図 27.1 に示すように、次の BIG-IP システムオブジェクトを設定します。

- 名前が **my_radius_monitor** の RADIUS モニタ
- 名前が **system_auth_name1**、IP アドレスおよびポートが **10.1.1.99:1645** の RADIUS サーバオブジェクト
- 名前が **system-auto** で、RADIUS サーバオブジェクトを参照する RADIUS 構成オブジェクト
- 名前が **radius_pool** で、RADIUS モニタを参照し、2 つのプールメンバ **10.1.1.10:1812** と **10.1.1.12:1645**）を持つプール。
  ポート **1812** は、RADIUS サーバの予約ポート番号である点に注意してください。
- 名前が **radius_virtual_server** で、プール **radius_pool** を参照し、RADIUS サーバオブジェクトと同じ IP アドレスとポートを使用する仮想認証サーバ。
  このバーチャルサーバは、プール内の各種 RADIUS サーバと同一の VLAN に定義される点に注意してください。

上記ファイル例と同様にして **bigip.conf** ファイルへのエントリの追加が終了すると、このバーチャルサーバを仮想リモート認証サーバとして使用できるようになります。

28

ペアトンネリングの実装

- ペアトンネリングの実装
- クライアント側 BIG-IP の設定
- サーバ側 BIG-IP の設定
- データ圧縮の統計情報の表示

ペアトンネリングの実装

2つのBIG-IPの間が広域ネットワーク（WAN）で分離されている場合、2つのBIG-IP間のデータ転送を最適化することができます。この最適化は、*トンネル*と呼ばれる特殊な最適化経路を2つのBIG-IPの間に作成することにより実現できます。いずれかのBIG-IPがこのトンネルを使用して他方のBIG-IPにデータを送信する場合、データは、圧縮品質と速度が最適になるように圧縮されます。

また、トンネルを通過するトラフィックの暗号化と復号化を行うように2つのBIG-IPを設定することにより、WANを横切るトラフィックのセキュアな接続を保証することもできます。

これらの最適化は、ペアトンネリングというBIG-IPの設定を行うことにより実装できます。

ペアトンネリングについて

*ペアトンネリング*設定では、LTMを実行する2つのBIG-IPが広域ネットワーク（WAN）の両側に配置され、WANを横切るデータ転送の最適化を目的として、これらのBIG-IPの間でトンネルが確立されます。図28.1は、この設定を示します。

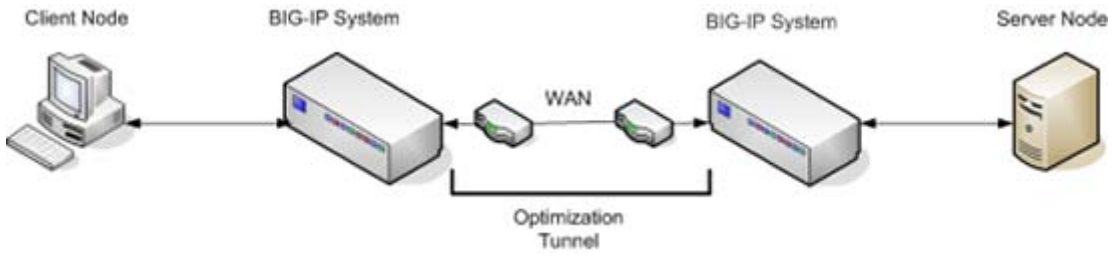

図28.1 *ペアトンネリング設定の例*

クライアント側BIG-IPは、サーバノードにあるデータの要求をWAN経由で開始するクライアントノードに最も近いBIG-IPです。***サーバ側BIG-IP***は、要求を処理するサーバノードに最も近いBIG-IPです。

ペアトンネリングの設定には、設定ユーティリティまたは**bigpipe**ユーティリティを使用できます。

データ圧縮について

ペアトンネリングが設定されている場合、BIG-IP は、FTP、Telnet、HTTP など、すべての TCP 関連のプロトコルに関するデータおよびヘッダを圧縮します。また、ペアトンネリング設定では、ダイナミックに生成されたデータも圧縮できます。

BIG-IP が実際に使用する圧縮方式は、ユーザ設定とパフォーマンス最適化の組み合わせによって異なります。ペアトンネリングが設定されている場合にBIG-IPが使用可能な圧縮方式は以下のとおりです。

- **deflate**
  高品質の圧縮アルゴリズムです。通常、ハードウェア高速化を併用していない場合、**lzo** アルゴリズムより低速です。**deflate** アルゴリズムは、比較的低速なリンク（たとえば、T1、DS3 リンクなど）での良好な圧縮を達成するために最適です。
- **lzo**
  高速、中品質、低遅延の圧縮アルゴリズムです。
  Lempel-Ziv-Oberhumer（**lzo**）アルゴリズムは、対話型プロトコル（Telnet など）や圧縮の効きやすい広帯域幅のプロトコル（データレプリケーションなど）に最適です。
- **adaptive**
  トラフィックの状況変化に合わせて最適なアルゴリズム（**deflate**、**lzo**、または **off**）を選択する圧縮方式です。**adaptive** 方式は、デフォルトの圧縮方式であり、推奨される方式です。
- **off**
  圧縮方式が **off** に設定されている場合、2 つの BIG-IP 間を通過するトラフィックの圧縮は行われません。この選択肢は、ストリーミングメディア（すでに圧縮済み）や暗号化プロトコルなど、圧縮できないプロトコルに最適です。

圧縮方式は、2 つの BIG-IP で同じに設定する必要があります。ただし、いずれかが **adaptive** 圧縮方式に設定されている場合は除きます。たとえば、次のようになります。

- 片側が **deflate** 方式を使用し、もう一方が **lzo** 方式を使用するように設定した場合、現在トンネルを通過している接続はすべてリセットされ、以降のトラフィックは許可されません。
- 片側が **deflate** 方式を使用し、もう一方が **adaptive** 圧縮を使用するように設定した場合、データは **deflate** 方式を使用して圧縮されます。
- 両方が **adaptive** 方式を使用するように設定した場合（すなわちデフォルト設定の場合）、トラフィック状況に応じて、**deflate**、**lzo**、または **off** のいずれかが使用されます。この設定が推奨されます。

◆ 警告

BIG-IP が iSession トンネル経由で送信するデータは、他のメカニズムによって圧縮や暗号化がすでに行われたものではないことを確認する必要があります。トンネルをターゲットにしたデータがすでに最適化されている場合、それ以上の最適化はできないだけではなく、悪影響を生じる可能性もあります。

準備

ペアトンネリング設定を開始する前に、以下の注記事項を考慮する必要があります。

- 作成するすべてのローカルトラフィック管理オブジェクト（プール、プロファイル、バーチャルサーバなど）は、現在の管理パーティションに作成されます。そのため、各BIG-IP上の現在の管理パーティションが適切に設定されていることを確認する必要があります。
- プール、プロファイル、バーチャルサーバの作成を許可するユーザロールがユーザアカウントに割り当てられていることが必要です。
- ペアトンネリング設定はルートドメインを完全にサポートします。すなわち、ペアトンネリング設定の一部として作成するバーチャルサーバおよびプールメンバをデフォルト以外のルートドメインに配置することができます。

これらのトピックの詳細については、『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください。

クライアント側 BIG-IP の設定

クライアント側の BIG-IP の設定手順では、以下の作業をこの順序で実行する必要があります。

- エンドポイントプールを作成し、サーバ側の BIG-IP 上のバーチャルサーバに割り当てる予定のアドレスと同じ IP アドレスを持つメンバを 1 つ作成します（サーバ側の BIG-IP 上のバーチャルサーバの作成については、「*サーバ側 BIG-IP の設定*」（28-9 ページ）を参照してください）。
- 上記エンドポイントプールを参照するカスタムiSessionプロファイルを作成します。
- トラフィックを処理するバーチャルサーバを作成し、これに上記 iSession プロファイルと SSL プロファイルを割り当てます。

以降のセクションでは、設定ユーティリティを使用してこれらの作業を実行する方法を説明します。

クライアント側エンドポイントプールの作成

クライアント側 BIG-IP の設定における最初の作業は、クライアント側 BIG-IP 上のエンドポイントプールの作成です（例 : **clientside_endpoint_pool**）。このプールは、2 つの BIG-IP 間のトンネルのエンドポイントとして機能します。プールには、1 つのプールメンバが含まれます。このプールメンバはサーバ側のバーチャルサーバ（IP アドレスおよびサービス）です。

クライアント側BIG-IP上のエンドポイントプールを作成するには

1. ナビゲーションメニューの [Main] タブで、[**Local Traffic**] を展開して [**Pools**] をクリックします。
   BIG-IP 上にあるプールのリストが表示されます。
2. 右上の [**Create**] をクリックします。
   [New Pool] 画面が表示されます。

   ***注 : [Create]** ボタンをクリックできない場合は、プールを作成する権限が付与されていません。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
3. [**Name**] ボックスに、プールの名前（**clientside_endpoint_pool** など）を入力します。
4. [**New Members**] 設定で、以下の作業を行います。
   a) [**New Address**] をクリックします。
   b) [**Address**] ボックスに、サーバ側 BIG-IP 上のバーチャルサーバに割り当てる仮想アドレスを入力します。
   c) [**Service Port**] リストでサービスを指定します。
   d) [**Add**] をクリックします。
   指定した IP アドレスとサービスがプールメンバとしてプールに追加されます。
5. [**Finished**] をクリックします。

クライアント側 iSession プロファイルの作成

次に、クライアント側 BIG-IP 上のカスタム iSession プロファイルを作成します。iSession プロファイルは、BIG-IP で使用する圧縮のタイプを指定するとともに、先に作成したエンドポイントプールを指定します。

クライアント側のカスタム iSession プロファイルを作成するには

1. ナビゲーションメニューの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   BIG-IP 上にある HTTP プロファイルのリストが表示されます。
2. [Services] メニューから、[iSession] を選択します。
3. 右上の [**Create**] をクリックします。
   [New iSession Profile] 画面が開きます。

   注 : [Create] *ボタンをクリックできない場合は、プロファイルを作成する権限が付与されていません。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
4. [**Name**] ボックスに、プロファイルの名前（**clientside_isession_profile** など）を入力します。
5. [**Mode**] が [**Enabled**] に設定されていることを確認します。
6. [**Compression**] リストから、BIG-IP で使用する圧縮アルゴリズムを選択します。

   注 : *選択する圧縮アルゴリズムは、サーバ側の BIG-IP で選択するタイプと一致する必要があります。ただし、いずれかの BIG-IP が* ***adaptive*** *に設定されている場合を除きます。デフォルト値は* ***adaptive*** *です。*
7. [**Port Transparency**] および [**Reuse Connection**] が [**Enabled**] に設定されていることを確認します。
8. [**Target Virtual**]が[**None**]に設定されていることを確認します。
9. [**Endpoint Pool**] リストから、先にサーバ側 BIG-IP で作成したエンドポイントプールを選択します。この例では、プール名は **clientside_endpoint_pool** です。
10. [**Finished**] をクリックします。

クライアント側バーチャルサーバの作成

クライアント側 BIG-IP をセットアップするための次の作業は、バーチャルサーバの作成です。このバーチャルサーバの目的は、広域ネットワーク（WAN）の反対側にある特定のサーバノードまたはサブネットを宛先とするクライアントトラフィックをキャプチャすることです。バーチャルサーバでは、そのトラフィックを iSession トンネル経由で転送して最適化を行います。

図 28.2 は、パケットの宛先 IP アドレスに基づいたクライアント側仮想アドレス設定の例を示します。

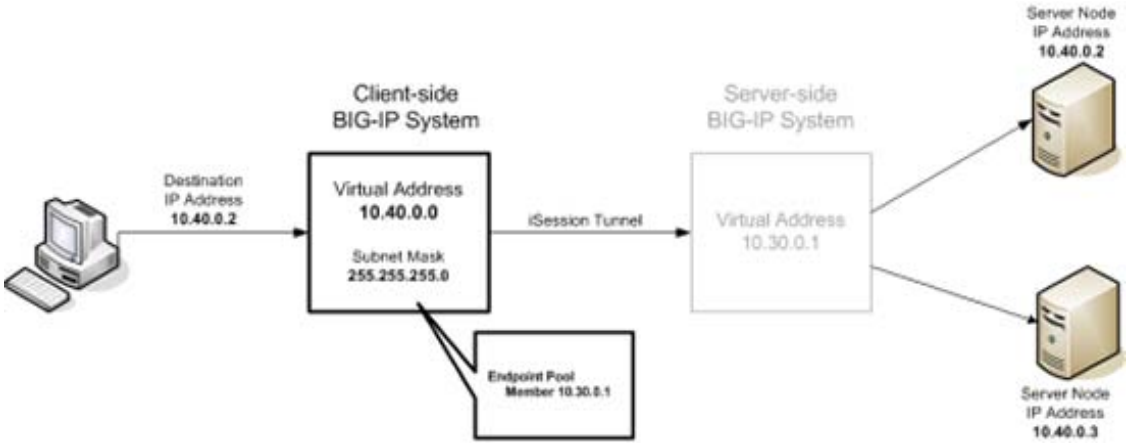

***図 28.2** クライアント側仮想アドレス設定の例*

指定する仮想アドレスがサブネットを表すアドレスの場合、ペアトンネリング設定内の BIG-IP は、宛先サーバが配置されているサブネット全体に向けたトラフィックを最適化します。

バーチャルサーバを作成する際には、以下のプロファイルを参照するように設定します。

- **デフォルトの TCP 最適化プロファイル**
  バーチャルサーバが 2 つのデフォルト TCP 最適化プロファイルを参照するように設定することにより、ローカル TCP トラフィックと広域 TCP トラフィックの両方を処理する場合の最適なシステムパフォーマンスが保証されます。
- **デフォルトの Server SSL プロファイル**
  BIG-IP では、**serverssl** という名前のデフォルトプロファイルを提供しています。このプロファイルは、サーバ側の SSL 処理を有効化します。**serverssl** プロファイルにより、クライアント側の BIG-IP からサーバ側の BIG-IP に送信されたトラフィックが確実に暗号化されます。
- **カスタム iSession プロファイル**
  このプロファイルは、前の手順で作成したのもであり、先に作成したエンドポイントプールを指定し、サーバ側のバーチャルサーバアドレスを参照します。

◆注

オプションで、RAM キャッシュ機能を有効にすることができます。その結果、WAN の反対側のバックエンドサーバへの接続を必要とせずに、クライアント側の BIG-IP が一部のクライアント要求を処理できます。

クライアント側バーチャルサーバを作成するには

1. ナビゲーションメニューの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   BIG-IP 上にあるバーチャルサーバのリストが表示されます。
2. 右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   ***注:** [Create] ボタンをクリックできない場合は、バーチャルサーバを作成する権限が付与されていません。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**clientside_virtual_server** など）を入力します。
4. [**Destination**] 設定で、次の作業を行います。
   a) 指定したアドレスが特定のサーバノードを表すか、サブネットを表すかに応じて、それぞれ [**Host**] または [**Network**] をクリックします。
   b) [**Address**] ボックスに、宛先の IP アドレスを入力します。このアドレスは、クライアントノードが要求を送信する特定のサーバノードの宛先 IP アドレスであるか、サーバノードが配置されたサブネットに一致するアドレスであることが必要です。
   c) 手順 4.a. で [**Network**] を選択した場合は、[**Mask**] ボックスにサブネットマスクを入力します。
5. [**Service Port**] リストから、サービスとして [**HTTP**] または [***All Ports**] などを選択します。
   バーチャルサーバは、この選択に応じて、指定されたポート上のトラフィックをリスニングします。特定のサービスポート（[**HTTP**]）などを選択すると、バーチャルサーバは他のすべてのトラフィックタイプを無視します。
6. [**Configuration**] リストから、[**Advanced**] を選択します。
7. [**Type**] の値が [**Standard**] であることを確認します。
8. [**Protocol Profile (Client)**] リストから、[**tcp-lan-optimized**] を選択します。
9. [**Protocol Profile (Server)**] リストから、[**tcp-wan-optimized**] を選択します。
10. [**SSL Profile (Client)**] リストでは、デフォルト値の [**None**] をそのまま使用します。
11. [**SSL Profile (Server)**] リストから、[**serverssl**] を選択します。
    これにより、BIG-IP が SSL 接続を開始し、トンネルからトラフィックを送信します。

12. [**VLAN Traffic**] リストから、[**All VLANS**] を選択します。
13. [**iSession Profile**] 設定では、以下の手順を実行します。
    a) 左側のリストから、先にこの BIG-IP 上に作成したカスタム iSession プロファイルの名前を選択します。この例では、**clientside_isession_profile** です。
    b) [**Context**] リストから、[**Server**] を選択します。
    [**Server**] を選択すると、トンネルのローカルエンドポイントは、作成しているバーチャルサーバのサーバ側にあることが指定されます。
14. [**Finished**] をクリックします。

サーバ側 BIG-IP の設定

ペアトンネリングのサーバ側の BIG-IP の設定には、単にバーチャルサーバの作成のみが必要です。このバーチャルサーバの目的は、サーバのプールに対する接続の負荷分散ではなく、サーバ側の BIG-IP の後方にあるローカルエリアネットワーク（LAN）にトラフィックを確実に転送することです。

このバーチャルサーバには、クライアント側のバーチャルサーバがルーティング可能な任意のIPアドレスを割り当てることができます。標準的な設定では、このアドレスは実際の宛先サーバノードと同じサブネットに配置されます。上述のように、このサーバ側バーチャルサーバに割り当てるアドレスは、クライアント側の BIG-IP 上に設定したエンドポイントプールの単一メンバとしても指定されています。

図 28.3 は、クライアント側の仮想アドレス設定に基づいたサーバ側仮想アドレス設定の例を示します。

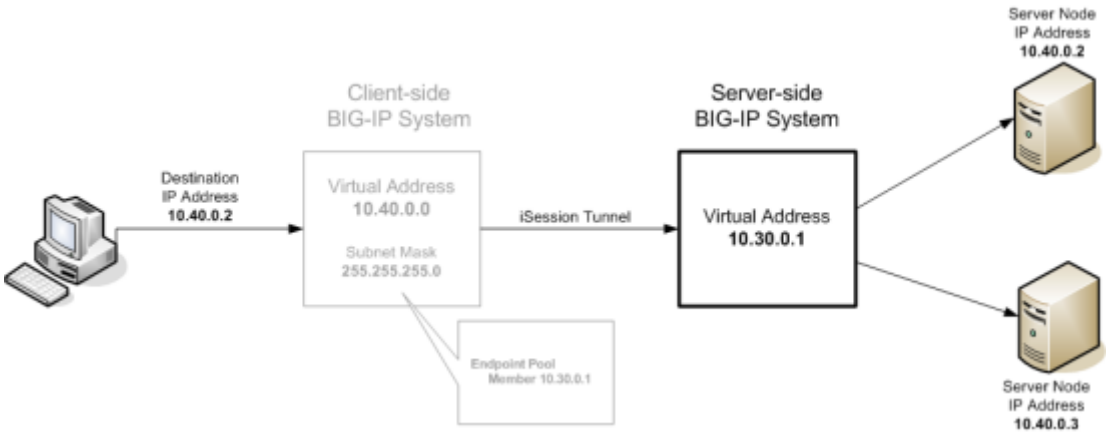

図 28.3 サーバ側バーチャルサーバ設定の例

サーバ側 BIG-IP 上のバーチャルサーバは、以下のプロファイルを参照します。

- **デフォルトの TCP 最適化プロファイル**
  バーチャルサーバが 2 つのデフォルト TCP 最適化プロファイルを参照するように設定することにより、ローカル TCP トラフィックと広域 TCP トラフィックの両方を処理する場合の最適なシステムパフォーマンスが保証されます。
- **デフォルトの Client SSL プロファイル**
  BIG-IP では、**clientssl** という名前のデフォルトプロファイルを提供しています。このプロファイルは、クライアント側の SSL 処理を有効化します。**clientssl** プロファイルにより、クライアント側の BIG-IP からサーバ側の BIG-IP に送信されたトラフィックの認証および暗号化が確実に実行されます。
- **デフォルトの iSession プロファイル**
  このプロファイルをバーチャルサーバに割り当てることにより、ペアトンネリング設定のサーバ側エンドポイントが実装されます。

◆注

サーバ側 BIG-IP については、エンドポイントプールやカスタム iSession プロファイルを作成する必要はありません。

サーバ側バーチャルサーバの作成

以下の手順を使用して、サーバ側のバーチャルサーバを作成できます。

サーバ側バーチャルサーバを作成するには

1. ナビゲーションメニューの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   BIG-IP 上にあるバーチャルサーバのリストが表示されます。
2. 右上の [**Create**] をクリックします。
   [New Virtual Server] 画面が開きます。

   注: *[Create] ボタンをクリックできない場合は、バーチャルサーバを作成する権限が付与されていません。ユーザアカウントに適切なユーザロールを割り当てておく必要があります。*
3. [**Name**] ボックスに、バーチャルサーバの名前（**serverside_forwarding_virtual_server** など）を入力します。
4. [**Destination**] 設定で、次の作業を行います。

   a) [**Host**] をクリックします。

   b) [**Address**] ボックスに、IP アドレスを入力します。
   重要: *この IP アドレスは、クライアント側 BIG-IP 上のエンドポイントプールを作成する際に指定したプールメンバアドレスと一致する必要があります。*
5. [**Service Port**] リストから、[***All Ports**] を選択します。
   詳細については、「*サービスポートの指定*」（28-11 ページ）を参照してください。
6. [**Configuration**] リストから、[**Advanced**] を選択します。
7. [**Type**] の値が [**Standard**] であることを確認します。
8. [**Protocol Profile (Client)**] リストから、[**tcp-wan-optimized**] を選択します。
   この設定はオプションです。
9. [**Protocol Profile (Server)**] リストから、[**tcp-lan-optimized**] を選択します。
10. [**SSL Profile (Client)**] リストから、[**clientssl**] を選択します。
    これにより、トンネルから着信するトラフィック用に BIG-IP が SSL 接続を終端します。
11. [**SSL Profile (Server)**] が [**None**] に設定されていることを確認します。
12. [**VLAN Traffic**] リストから、[**All VLANS**] を選択します。

13. [**iSession Profile**] 設定では、以下の手順を実行します。

    a) 左側のリストから、[**isession**] を選択します。

    b) [**Context**] リストから [**Client**] を選択します。
    [**Client**] を選択すると、トンネルのローカルエンドポイントは、作成しているバーチャルサーバのクライアント側にあることが指定されます。

14. [**Finished**] をクリックします。

サービスポートの指定

サーバ側のバーチャルサーバを設定する場合、[**Service Port**] を [***All Ports**] に設定することをお勧めします。その場合、実際にサーバ側のバーチャルサーバがリスニングするサービスポートは、クライアント側 BIG-IP でのポート透過性の設定に応じて変化します。***ポート透過性***は、クライアント側の iSession プロファイル内で設定する機能です。

表 28.1 は、クライアント側 BIG-IP での [**Port Transparency**] 設定がサーバ側バーチャルサーバの挙動にどのように影響するかを示します。

クライアント側のポート透過性の設定	サーバ側バーチャルサーバがリスニングする対象	例
Enabled （デフォルト設定）	クライアント側バーチャルサーバでの設定と同じサービスポート	クライアント側のサービスポートが **HTTP** に設定されている場合、サーバ側のバーチャルサーバはポート **80** をリスニングします。
Disabled	iSession ポート **3701**	クライアント側のサービスポートが **HTTP** に設定されている場合、サーバ側のバーチャルサーバはポート **3701** をリスニングします。

***表 28.1** クライアント側の **[Port Transparency]** 設定によるサーバ側バーチャルサーバへの影響*

データ圧縮の統計情報の表示

ペアトンネリング設定の作成が終了し、2 つの BIG-IP が WAN 経由のトラフィックを処理している場合、クライアント側 BIG-IP でのデータ圧縮の統計情報を表示することができます。

データ圧縮の統計情報を表示するには

これらの統計情報を表示するには、以下のように、クライアント側の BIG-IP で **bigpipe** ユーティリティを使用します。

```
bp> profile isession isession show
```

元のデータ量と最適化されたデータ量の両方の統計が表示されます。

29

ASMおよびWAによるHTTPトラフィックのセキュリティ 保護と高速化

- 設定タスクの概要
- BIG-IP LTM での基本的な設定の完了
- BIG-IP LTM での初期設定タスクの実行
- WebAccelerator 用のアプリケーションプロファイル の作成
- Application Security Manager のセキュリティポリシー へのWebAcceleratorアプリケーションプロファイルの割り当て
- Application Security ManagerのDeployment Wizard の実行

設定タスクの概要

ここで説明する実装は、***BIG-IP***® Application Security Manager および ***BIG-IP***® WebAccelerator™ を同じバーチャルサーバ上で実行するための設定タスクを示します。

この実装において、システムが接続をセキュリティで保護し、アプリケーションの HTTP トラフィックを高速化できるようにするには、以下のタスクを実行する必要があります。

- **BIG-IP LTM での基本的な設定の完了**
  この実装を開始する前に、BIG-IP LTM での基本的な設定要件を完了する必要があります。詳細については、「*BIG-IP LTM での基本的な設定の完了*」（29-2 ページ）を参照してください。
- **BIG-IP LTM での初期設定タスクの実行**
  Application Security Manage および WebAccelerator を同じバーチャルサーバ上で実行するための BIG-IP LTM の準備として、初期設定タスクを完了する必要があります。詳細については、「*BIG-IP LTM での初期設定タスクの実行*」（29-3 ページ）を参照してください。
- **WebAccelerator 用のアプリケーションプロファイルの作成**
  アプリケーションプロファイルは、WebAccelerator がアプリケーションのトラフィックの高速化を開始するために必要な基本情報のすべてを提供します。詳細については、「*WebAccelerator 用のアプリケーションプロファイル の作成*」（29-7 ページ）を参照してください。
- **Application Security Manager の Deployment Wizard の実行**
  Deployment Wizard は、アプリケーションのセキュリティプロファイルを最初に構築し、展開するために必要な基本タスクを自動化します。詳細については、「*Application Security Manager の Deployment Wizard の実行*」（29-13 ページ）を参照してください。

BIG-IP LTM での基本的な設定の完了

Application Security Manage および WebAccelerator を同じバーチャルサーバ上で実行するために必要なプロセスを開始する前に、BIG-IP LTM 上で基本的な設定タスクを完了しておく必要があります。以下のタスクの完了が必要です。

- **Application Security Manager および WebAccelerator 用のライセンス供与とプロビジョニング**
  詳細については、『***BIG-IP® Systems: Getting Started Guide***』を参照してください。
- **バーチャルサーバの設定**
  詳細については、『***Configuration Guide for BIG-IP® Local Traffic Management***』を参照してください。
- **名前解決（DNS またはホストファイルのエントリ）の設定**
  詳細については、『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください。

BIG-IP LTM での初期設定タスクの実行

BIG-IP LTM での基本設定タスクを実行した後、Application Security Manager と WebAccelerator の両方を同じバーチャルサーバ上で実行するための準備に必要な初期設定タスクを完了することができます。

BIG-IP LTM の初期設定には以下のタスクがあります。

- **Application Security Manager および WebAccelerator 用の HTTP クラスプロファイルの作成**
  HTTP クラスプロファイルでは、HTTP ヘッダ、Cookie、ホスト、パス、その他の HTTP プロパティを使用して、システムがセキュリティと高速化を適用する HTTP トラフィックを指定します。詳細については、後述の「*HTTP クラスプロファイルの作成*」を参照してください。
- **バーチャルサーバおよびプールの定義**
  バーチャルサーバは、Web アプリケーションをホストする 1 つまたは複数のプールへのトラフィックの負荷分散を実行します。プールを構成するメンバは、Application Security Manager で保護する Web アプリケーションリソースをホストし、トラフィックを WebAccelerator で高速化するサーバです。詳細については、「*BIG-IP LTM でのバーチャルサーバとプールの定義*」（29-4 ページ）を参照してください。
- **NTP（Network Time Protocol）サーバの設定**
  システムでキャッシュが正しく維持され、設定が同期するには、アプリケーションサーバ上の時間と、BIG-IP 上の時間が同じであることが必要です。詳細については、「*NTP サーバの定義*」（29-6 ページ）を参照してください。

HTTP クラスプロファイルの作成

BIG-IP LTM が Application Security Manager と WebAccelerator を実行するための準備に必要な最初のタスクは、HTTP クラスプロファイルの作成です。HTTP クラスプロファイルでは、HTTP ヘッダ、Cookie、ホスト、パス、その他の HTTP プロパティを使用して、システムがセキュリティと高速化を適用する HTTP トラフィックを指定します。この実装では、Application Security Manager と WebAccelerator の両方を有効化する HTTP クラスプロファイルを 1 つ作成します。

◆ 重要

HTTP クラスプロファイルのアプリケーションセキュリティを有効にすると、Application Security Manager 用の Web アプリケーション設定とデフォルトのセキュリティプロファイルが自動的に作成されます。

HTTP クラスプロファイルを作成するには

1. ナビゲーションペインの [Main] タブで [**Application Security**] を展開し、[**Classes**] をクリックします。
   [HTTP Class] 画面が開きます。

2. [作成] ボタンをクリックします。
   [New HTTP Class Profile] 画面が開きます。
3. [**Name**] ボックスに、HTTP クラスプロファイルの一意な名前を入力します。
4. [**Parent Profile**] リストから、[**httpclass**] を選択します。
5. [Configuration] 領域で、[Custom] ボックス（右側）のチェックマークをオンにして [**WebAccelerator**] 設定を有効にし、リストから [**Enabled**] を選択します。
6. [**Application Security**] 設定も有効化されていることを確認します。
7. [**Finished**] ボタンをクリックします。
   新しい HTTP クラスプロファイルが追加され、[HTTP Class Profiles] 画面が表示されます。

HTTP クラスプロファイル設定時の重要な考慮事項

設定ユーティリティでは、ナビゲーションペインの複数のセクションから HTTP クラスプロファイルを作成することができます。HTTP クラスプロファイルを [**Local Traffic**] セクションから作成する場合、デフォルトでは [**WebAccelerator**] 設定と [**Application Security**] 設定の両方が無効になります。したがって、HTTP クラスによるトラフィックの高速化とセキュリティ保護を実施する場合には、これらの設定の両方を明示的に有効化する必要があります。HTTP クラスプロファイルを設定ユーティリティの [**Application Security**] セクションまたは [**WebAccelerator**] セクションから作成する場合、HTTP クラスプロファイル設定において、それぞれの設定がデフォルトで有効化されます。この場合には、対応する設定の 1 つだけを明示的に有効化する必要があります。

BIG-IP LTM でのバーチャルサーバとプールの定義

次に実行するタスクは、バーチャルサーバとプールの定義です。定義の一部として、前の手順で作成した HTTP クラスプロファイルをバーチャルサーバに関連付けます。すると、バーチャルサーバでは、関連付けられた HTTP クラスプロファイルでの設定に基づいて、受信トラフィックの処理とルーティングが行われます。プールは、クライアントがアクセスする Web アプリケーションのコンテンツをホストします。

◆注

*以下の手順は、バーチャルサーバとプールの基本的な設定の概要のみを示したものです。バーチャルサーバ、プール、その他のローカルトラフィックコンポーネントの詳細については、『**Configuration Guide for BIG-IP® Local Traffic Management**』を参照してください。*

バーチャルサーバおよびプールを設定するには

1. ナビゲーションペインの [Main] タブで [**Local Traffic**] を展開し、[**Virtual Servers**] をクリックします。
[Virtual Servers list] 画面が開きます。
2. [**Create**] ボタンをクリックします。
[New Virtual Server] 画面が開きます。
3. [General Properties] 領域で、[**Name**] 設定にバーチャルサーバの一意の名前を入力します。
4. [**Destination**] 設定の [**Host**] ボタンをクリックし、[**Address**] ボックスに IP アドレスを入力します。
5. [**Service Port**] 設定には、アプリケーションに関連したサービスポートを入力します。たとえば、HTTP の場合、ポートは **80** です。または、サービスタイプをリストから選択することもできます。
6. [**State**] リストから、[**Enabled**] を選択します。
7. [Configuration] 領域の上の [**Advanced**] を選択します。
画面が更新され、追加の設定オプションが表示されます。
8. [Configuration] 領域で、[**HTTP Profile**] リストから [**http-acceleration**] を選択します。

   ***重要**: [http-acceleration] サービスプロファイルの RAM キャッシュの有効化を維持し、[Minimum Object Size]、[Maximum Object Size]、[URI Caching]、[Ignore Headers] の RAM キャッシュのデフォルト設定は一切変更しないことを強くお勧めします。これらを変更すると、BIG-IP WebAccelerator がサイトの HTTP トラフィックを管理する方法に悪影響を及ぼします。*
9. [**Port Translation**] で設定が有効化されている（チェックマークがオンになっている）ことを確認します。

   ***重要**: バーチャルサーバの [Port Translation] 設定が無効化されている場合、WebAccelerator はトラフィックを正しく高速化できません。*
10. [**SNAT Pool**] 設定で、[**Auto Map**] を選択します。
11. [Resources] 領域で、[**HTTP Class Profiles**] 設定の [**Available**] リストから作成した Application Security Manager/WebAccelerator 対応の HTTP クラスプロファイルを選択し、移動ボタン（[<<]）をクリックして、プロファイルを [**Enabled**] リストに追加します。
12. [**Default Pool**] 設定の隣の追加ボタン（[+]）をクリックします。
[New Pool] 画面が開きます。
13. [Configuration] 領域で、[**Name**] 設定にプールの一意の名前を入力します。
14. [**Health Monitors**] 設定で、[**Available**] リストから**ヘルスモニタを 1 つまたは複数選択し、**移動ボタン（[<<]）をクリックしてモニタを [**Available**] リストに追加します。

15. [Resources] 領域で、[**Load Balancing Method**] リストから負荷分散オプションを選択します。
16. [**Priority Group Activation**] 設定がデフォルトの [**Disabled**] であることを確認します。
17. [**New Members**] 設定で [**New Address**] を選択し、[**Address**] および[**Service Port**]ボックスにプールメンバのアドレスおよびポートを入力します。または、[**Node List**] を選択し、[**New Members**] リストに追加するノードを選択することもできます。
18. [**Add**] ボタンをクリックします。
19. [**Finished**] をクリックします。
画面が更新され、[New Virtual Server] 画面に戻ります。この画面の [**Default Pool**] リストには新しいプールが表示されています。
20. [**Finished**] をもう一度クリックします。
設定が更新され、[Virtual Server] リスト画面が表示されます。この画面には、作成したバーチャルサーバが表示されています。

NTP サーバの定義

次に、NTP（Network Time Protocol）サーバを定義します。***NTP*** は、ネットワーク経由で設定された NTP サーバと、クロックを同期させるプロトコルです。この同期により、BIG-IP LTM でキャッシュが正しく維持されるとともに、設定の変更が同期されることが保証され、WebAccelerator の対向設置オプションが実現可能になります。

NTP サーバを定義するには

1. ナビゲーションペインの [Main] タブで、[**System**] を展開して [**Configuration**] をクリックします。
[General] 画面が表示されます。
2. [Device] メニューから [NTP] を選択します。
[NTP] 画面が表示されます。
3. [Time Server List] の [**Address**] ボックスに、NTP サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
4. [**追加**] ボタンをクリックして、サーバをリストに追加します。
5. [**Update**] をクリックして、変更を保存します。

WebAccelerator 用のアプリケーションプロファイルの作成

ローカルエリアネットワークをセットアップするための最初の一連のタスクが完了したら、次は WebAccelerator 用のアプリケーションプロファイルを作成します。*アプリケーションプロファイル*は、WebAccelerator がサイトの Web アプリケーションへの要求を適切に処理するために必要とする主要情報を提供します。アプリケーションプロファイルの作成は以下のタスクで構成されます。

- アプリケーションへのトラフィックを管理するための高速化ポリシーの選択
- ホストマップの計画と定義
- アプリケーションプロファイルの検証

高速化ポリシーの選択

アプリケーションプロファイルの作成プロセスを開始するには、最初に、アプリケーションに関連付ける高速化ポリシーを決定する必要があります。1 つの選択肢は、特定のアプリケーションパブリッシャーに関連付けられている事前定義済みの高速化ポリシーを選択するという方法です。

特定のアプリケーションパブリッシャー専用の高速化ポリシーの使用を望まない場合には、2 つの汎用事前定義済み高速化ポリシーのいずれかを使用できます。これらは 2 つとも、Java 2 Platform Enterprise Edition（J2EE）アプリケーションを使用するサイトのほとんどで良好に動作します。

- **Level 1 Delivery**
  この事前定義済み高速化ポリシーは、HTML バージョン 2.0 に準拠します。この高速化ポリシーの場合、WebAccelerator は以下のように動作します。
  - HTML ページに対するすべての要求を、コンテンツ発信元の Web サーバに送信します。
  - HTTP **Cache-Control** リクエストヘッダに含まれる no-cache 指示子を無視し、発信元 Web サーバから受信する cache response 指示子を使用します。

- **Level 2 Delivery**
  この事前定義済み高速化ポリシーは、HTML バージョン 3.0 以降に準拠します。この高速化ポリシーの場合、WebAccelerator は以下のように動作します。
  - HTML ページをキャッシュし、**0** のライフタイム設定を割り当てます。これは、WebAccelerator に対して、条件付き GET でそのコンテンツの以降の要求を行うことにより、最新のコンテンツを提供するように求めます。
  - Intelligent Browser Referencing 機能を documents および includes のみに使用します。

- HTTP **Cache-Control** リクエストヘッダに含まれる no-cache 指示子を無視し、発信元 Web サーバから受信する cache response 指示子を使用します。

WebAccelerator では、アプリケーション固有および汎用配信の高速化ポリシー以外に、対向設置と呼ばれる設置方法に固有の高速化ポリシーも提供しています。オプションの対象展開を設定する場合は、このオプションを選択できます。このオプションの詳細については、『***Configuration Guide for the BIG-IP® WebAccelerator™ System***』を参照してください。

事前定義の高速化ポリシーを使用できない特殊なアプリケーションがある場合には、***ユーザ定義の高速化ポリシー***を作成することにより、WebAccelerator の動作をカスタマイズできます。多くの場合、カスタマイズは、事前定義の高速化ポリシーをコピーし、これを必要に応じて変更することにより実施します。また、コンサルタントやベンダーなどが作成および認定し、暗号化した***署名付きの高速化ポリシー***をインポートするという選択肢もあります。

高速化ポリシー機能の詳細、ユーザ定義の高速化ポリシーの作成手順、署名付きの高速化ポリシーのインポート手順については、『***Policy Management Guide for the BIG-IP® WebAccelerator™ System***』を参照してください。

◆ ヒント

アプリケーションプロファイルの作成後、選択した高速化ポリシーはいつでも変更できます。

ホストマップの計画

WebAccelerator では HTTP リクエストを受信すると、リクエスト中のホストと***ホストマップ***上のホストを比較して、どのアプリケーションプロファイルを適用するかの決定を行います。システムがアプリケーションプロファイルに一致した後は、関連する高速化ポリシーを使用して要求を処理することができます。

ホストマップを作成する際、HTTP Host リクエストヘッダに示されるドメインを特定します。これらのドメインは、***requested host*** と呼ばれます。ホストマップに requested host 名を指定する場合、ワイルドカードとしてアスタリスク（*****）を使用し、その後にピリオドを続けることにより、ドメインの最初の文字を表すことができます。このワイルドカードは、複数のサブドメインを表すことができ、一度に複数のサブドメイン
を 1 つの発信元 Web サーバにマッピングすることができます。サイトに複数のサブドメインがある場合には、ワイルドカードを使用することにより、時間が節約されます。

◆ 注

*WebAccelerator は、マッピングされていないドメインの要求も管理できます。このようなリクエストはマップされていないリクエストと呼ばれます。詳細については、『**Configuration Guide for the BIG-IP® WebAccelerator™ System**』を参照してください。*

以下は、ワイルドカードを使用した有効な要求ホスト名の例を示します。

- ***.sales.siterequest.com** は、以下のようにマッピングします（宛先ホストはすべて同じ）。
  - **direct.sales.siterequest.com**
  - **marketing.sales.siterequest.com**
  - **marcom.marketing.sales.siterequest.com**
- ***siterequest.com** は、以下のようにマッピングします（宛先ホストはすべて同じ）。
  - **www.siterequest.com**
  - **engineering.siterequest.com**
  - **direct.sales.siterequest.com**
  - **marketing.sales.siterequest.com**
  - **marcom.marketing.sales.siterequest.com**
- ***.com** は、末尾が **.com** の受信ホストのすべてを 1 つの宛先ホストにマッピングします。
- ***.com** は、受信したすべての要求を 1 つの宛先ホストにマッピングします。

WebAccelerator が複数の要求ホスト名を 1 つの要求にマッピングできる場合、要求に最も近いホスト名が選択されます。以下のホスト名が定義されているとしましょう。

- **a.com**
- **www.a.com**
- ***.b.a.com**
- ***.a.com**

WebAccelerator がこれらの URL を含む要求を受信した場合、その要求は以下の要求ホストにマッピングされます。

- **www.a.com** に対する要求は、**www.a.com** にマッピングされ、***.a.com** にはマッピングされません。
- **a.com** に対する要求は、**a.com** にマッピングされます。
- **c.a.com** に対する要求および **b.a.com** に対する要求は、両方とも ***.a.com** にマッピングされます。
- **c.b.a.com** に対する要求は、***.b.a.com** にマッピングされます。

アプリケーションプロファイルを作成するには

1. ナビゲーションペインの [Main] タブで [**WebAccelerator**] を展開し、[**Applications**] をクリックします。
   新しいウィンドウに [Applications] 画面が表示されます。
2. [**Create**] ボタンをクリックします。
   [New Application] 画面が開きます。

3. [**Application Name**] ボックスに、アプリケーションの名前を入力します。
4. [**Description**] ボックスに説明を入力します（オプション）。
5. [**Central Policy**] リストから、関連するアプリケーションからの情報を要求する場合に WebAccelerator で使用する高速化ポリシーを選択します。オプションの対向設置を設定している場合には、**対向設置用**事前定義済み高速化ポリシーを選択することをお勧めします。このポリシーは、特に対向設置におけるコンテンツアセンブリの管理を目的としているためです。詳細については、
『***Configuration Guide for the BIG-IP® WebAccelerator™ System***』を参照してください。
6. 対向設置を使用する場合は、[**Remote Policy**] リストから、リモート WebAccelerator 用の高速化ポリシーを選択します。**Symmetric Deployment** を選択することをお勧めします。対向設置を使用しない場合、リモートポリシーは選択しないでください。
7. 画面の下部の [Hosts] セクションで、[**Add Host**] ボタンをクリックします。
8. [**Requested Host**] ボックスに、アプリケーションへのアクセス許可を与える各クライアントホストの有効なホスト名を入力します。
9. [**Save**] ボタンをクリックします。

アプリケーションプロファイルの検証

アプリケーションプロファイルの作成後、WebAccelerator が正しくデータを送信し、発信元 Web サーバからデータを受信できることを検証する必要があります。

アプリケーションプロファイルを検証するには

1. WebAccelerator から独立しており、Web ブラウザを実行可能なマシン上で、**hosts** ファイルを開き、Web サイトアプリケーションのアクセスに使用したホスト名を追加します。このホスト名は、設定したバーチャルサーバの IP アドレスを指定するものであることが必要です。

   注 : Microsoft® Windows® 2000 および Windows® XP マシンの場合、hosts ファイルの場所は C:\WINDOWS\system32\drivers\etc\hosts です。

   たとえば、**www.siterequest.com** ドメインの Web サイトをアクセスできる場合で、バーチャルサーバが IP アドレス **11.1.11.3** に配置されている場合、ブラウザ実行しているマシンの **hosts** ファイルに以下の行を追加します。

   ```
   11.1.11.3   www.siterequest.com
   ```

   以降、**www.siterequest.com** の Web ブラウザマシンからのすべてのネットワークトラフィックは、バーチャルサーバに送信されます。

2. Web ブラウザマシンから、**www.siterequest.com** のページを要求します。

   ブラウザが発信元 Web サーバに直接アクセスしたなら受信していたはずのページが表示されます。ブラウザで要求がタイムアウトする場合、WebAccelerator が稼動していないか、WebAccelerator 上のポート **80** へのアクセスがファイアウォールでブロックされています。

3. **Access denied by intermediary. Domain not recognized.** という**エラー**を受信する場合、以下のタスクを実行します。

   - **hosts** ファイルが正しいことを検証します。
   - アプリケーションプロファイルのホストマップが正しいことを検証します。
   - 要求で使用したドメインがホストマップの要求ホストに一致しており、このホストマップは宛先ホストにマッピングしていることを検証します。

4. ホストマッピングを確認した後、変更や追加を行ったエントリのすべてを削除します。

Application Security Manager のセキュリティポリシーへのWebAcceleratorアプリケーションプロファイルの割り当て

Application Security Manager の Deployment Wizard を実行する前に、WebAcceleratorのアプリケーションプロファイルをセキュリティポリシーに割り当てる必要があります。複数のアプリケーションプロファイルが設定されている場合には、Application Security Manager の [Policy Properties] 画面で割り当てを変更できます。

WebAccelerator アプリケーションプロファイルをセキュリティポリシーに割り当てるには

1. Application Security ナビゲーションペインの [Main] タブで、[**Policies List**] をクリックします。
   [Security Policies] 画面が開きます。
2. 編集コンテキスト領域で、編集済みの Web アプリケーションとセキュリティポリシーが、更新予定のものに間違いないことを確認します。
3. [Security Policies] 領域の [Security Policy Name] カラムで、編集するセキュリティポリシーの名前をクリックします。
   [Security Policy Properties] 画面が開きます。
4. [Configuration] 領域の上の [**Advanced**] を選択します。
   画面が更新され、追加の設定オプションが表示されます。
5. [**WebAccelerator Cache Clear Settings**]オプションの[**Available WA Applications**] リストから、作成した WebAccelerator アプリケーションプロファイルを選択し、移動ボタン（<<）をクリックしてプロファイルを [**Assigned WA Applications**] リストに追加します。
6. [**Save**] ボタンをクリックします。

Application Security Manager の Deployment Wizard の実行

WebAccelerator のアプリケーションプロファイルの設定が完了すると、Application Security Manager のセキュリティポリシーの作成ができます。

新規 Web アプリケーションのセキュリティポリシーを構築するための最も効率的な方法は、Deployment Wizard を使用することです。Deployment Wizard は、セキュリティプロファイルを最初に構築し、展開するために必要な基本タスクを自動化します。 Deployment Wizard では、アプリケーションセキュリティを使用する標準的な環境を表す***展開シナリオ***を使用して、設定プロセスをガイドします。展開シナリオには、以下の種類があります。

- 本番環境の Web アプリケーション
- テスト環境の Web アプリケーション
- Web サービスアプリケーション
- システムが提供するアプリケーション対応のセキュリティポリシー

Deployment Wizard を開始するには

1. ナビゲーションペインの [Main] タブで [**Application Security**] を展開し、[**Web Applications**] をクリックします。
   [Web Applications] 画面が開きます。
2. 新しいWebアプリケーションの[**Set Language**]リンクをクリックします。
   [Select Deployment Scenario] 画面が開きます。
3. [Select Deployment Scenario] 領域で、展開シナリオを選択します。
   展開シナリオの詳細については、『***BIG-IP® Application Security Manager: Getting Started Guide***』を参照してください。
   このガイドは、F5 Prime Members Web サイト（**https://www.f5networks.co.jp/primemembers/**）から入手できます。
4. [**Run Deployment Wizard**] ボタンをクリックします。
   Application Security Manager の Deployment Wizard が開始されます。

30

PSMおよびWAによるHTTPトラフィックのセキュリティ保護と高速化

- 設定タスクの概要
- BIG-IP LTM での基本的な設定の完了
- BIG-IP LTM での初期設定タスクの実行
- WebAccelerator 用のアプリケーションプロファイルの作成
- Protocol Security Module 設定での HTTP セキュリティプロファイルの作成

設定タスクの概要

ここで説明する実装は、BIG-IP Protocol Security Module および BIG-IP WebAcceleratorを同じバーチャルサーバ上で実行するための設定タスクを示します。

この実装において、システムが接続をセキュリティで保護し、アプリケーションの HTTP トラフィックを高速化できるようにするには、以下のタスクを実行する必要があります。

- **BIG-IP LTM での基本的な設定の完了**
  この実装を開始する前に、BIG-IP LTM での基本的な設定要件を完了する必要があります。詳細については、「*BIG-IP LTM での基本的な設定の完了*」（30-2 ページ）を参照してください。

- **BIG-IP LTM での初期設定タスクの実行**
  Protocol Security Module および WebAccelerator を同じバーチャルサーバ上で実行するための BIG-IP LTM の準備として、初期設定タスクを完了する必要があります。詳細については、「*BIG-IP LTM での初期設定タスクの実行*」（30-3 ページ）を参照してください。

- **WebAccelerator 用のアプリケーションプロファイルの作成**
  アプリケーションプロファイルは、WebAccelerator がアプリケーションのトラフィックの高速化を開始するために必要な基本情報のすべてを提供します。詳細については、「*WebAccelerator 用のアプリケーションプロファイルの作成*」（30-7 ページ）を参照してください。

- **Protocol Security Module 設定での HTTP セキュリティプロファイルの作成**
  最後に、Protocol Security Module 設定において、カスタム HTTP セキュリティプロファイル作成し、これにWebAcceleratorアプリケーションプロファイルを関連付けます。詳細については、「*Protocol Security Module 設定での HTTP セキュリティプロファイルの作成*」（30-12 ページ）を参照してください。

BIG-IP LTM での基本的な設定の完了

Protocol Security Module および WebAccelerator を同じバーチャルサーバ上でセットアップし、実行するための設定タスクを開始する前に、BIG-IP LTM 上で基本的な設定タスクを実行する必要があります。以下のタスクを完了しておくことが必要です。

- **Protocol Security Module および WebAccelerator 用のライセンス供与とプロビジョニング**
  新規モジュールを BIG-IP に追加する場合、アドオンのライセンスキーをアクティベートします。また、新しいソフトウェア用にシステムのプロビジョニングも行います。***プロビジョニング***とは、ディスクストレージやメモリなど、システムリソースを再割り当てすることです。詳細については、『***BIG-IP® Systems: Getting Started Guide***』を参照してください。
- **最低 1 台の DNS サーバの設定**
  バーチャルサーバとアプリケーションの名前解決を有効にするために、DNS サーバを設定します。詳細については、『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください。
- **最低 1 台の NTP サーバの設定**
  WebAccelerator は、システムクロックの同期の維持を NTP プロトコルに依存しています。この同期により、WebAccelerator でキャッシュが正しく維持されるとともに、設定の変更が同期されることが保証され、対向設置オプションが実現可能になります。詳細については、『***TMOS™ Management Guide for BIG-IP® Systems***』を参照してください。

BIG-IP LTM での初期設定タスクの実行

BIG-IP LTM での基本設定タスクを実行した後、Protocol Security Module と WebAccelerator の両方を同じバーチャルサーバ上で実行するための準備に必要な BIG-IP LTM の初期設定タスクを完了することができます。Web アプリケーションに対して、Protocol Security Module がセキュリティをチェックし、WebAccelerator が高速化を行います。その Web アプリケーションを含む pool に対してバーチャルサーバが負荷分散を行います。また、バーチャルサーバは、それぞれのプロファイルを使用することにより、Protocol Security Module と WebAccelerator を接続するブリッジとなります。

この実装においては、以下の BIG-IP LTM 設定タスクを実行します。

- **WebAccelerator HTTP クラスプロファイルの作成**
  Protocol Security Module と WebAccelerator を設定するための最初の手順は、WebAccelerator クラスプロファイルの作成です。詳細については、「*WebAccelerator HTTP クラスプロファイルの作成*」（30-3 ページ）を参照してください。
- **HTTP サービスプロファイルの作成**
  WebAccelerator プロファイルを作成した後、カスタム HTTP サービスプロファイルを作成します。このプロファイルにより、受信 HTTP プロファイルに対して実行されるプロトコルセキュリティチェックが有効になります。詳細については、「*HTTP サービスプロファイルの作成*」（30-4 ページ）を参照してください。
- **バーチャルサーバおよびプールの作成**
  この手順では、HTTP クラスプロファイルおよび HTTP サーバプロファイルをバーチャルサーバに割り当て、1 つまたは複数のプールを定義するなど、バーチャルサーバの設定を行います。詳細については、「*BIG-IP LTM でのバーチャルサーバとプールの作成*」（30-5 ページ）を参照してください。

WebAccelerator HTTP クラスプロファイルの作成

BIG-IP LTM が Protocol Security Module と WebAccelerator を実行するための準備に必要な最初のタスクは、WebAccelerator HTTP クラスプロファイルの作成です。

WebAccelerator HTTP クラスプロファイルを作成するには

1. ナビゲーションペインの [Main] タブで [**WebAccelerator**] を展開し、[**Class Profiles**] をクリックします。
   [HTTP Class] 画面が開きます。
2. [**Create**] ボタンをクリックします。
   [New HTTP Class Profile] 画面が開きます。
3. [General Properties] 領域で、[**Name**] 設定に HTTP クラスプロファイルの一意の名前を入力します。
4. [**Parent Profile**] リストから、[**httpclass**] を選択します。

5. [Configuration] 領域で、[**WebAccelerator**] 設定が有効化されていることを確認します。
6. [**Finished**] ボタンをクリックします。
   新しい HTTP クラスプロファイルが追加され、[HTTP Class Profiles] 画面が表示されます。

HTTP サービスプロファイルの作成

次に、HTTP サービスプロファイルを作成します。HTTP サービスプロファイル（ローカルトラフィック設定）は、HTTP セキュリティプロファイル（Protocol Security Module 設定）を使用してスキャンし、プロトコル特有の脆弱性を調べます。セキュリティプロファイルの詳細については、「*Protocol Security Module 設定での HTTP セキュリティプロファイルの作成*」（30-12 ページ）を参照してください。

HTTP サービスクラスプロファイルを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Profiles**] をクリックします。
   [Profiles:Services:HTTP] 画面が開きます。
2. [**Create**] ボタンをクリックします。
   [New HTTP Profile] 画面が開きます。
3. [General Properties] 領域で、[**Name**] 設定にプロファイルの一意の名前を入力します。
4. [**Parent Profile**] で、新しいプロファイルの設定継承元の既存 HTTPプロトコルを選択します。デフォルト設定は[**http**]です。
5. [Settings] 領域の上の [**Custom**] チェックボックスをクリックします。
   個別の設定の編集モードが有効になります。
6. [**Protocol Security**] チェックボックスをオンにして、HTTP セキュリティチェックを有効にします。
7. 実際の設定での必要に応じて、画面のその他の設定項目を変更します。
8. [**Finished**] をクリックします。
   画面が更新され、新しい HTTP サービスプロファイルがリストに表示されます。

◆注

*HTTP サービスプロファイルの概要については、『**Configuration Guide for BIG-IP® Local Traffic Management**』を参照してください。*

BIG-IP LTM でのバーチャルサーバとプールの作成

次の設定タスクは、ローカルエリアネットワーク上のバーチャルサーバとプールの作成です。バーチャルサーバは、プロトコルセキュリティチェックや高速化ポリシーの適用など、着信トラフィックの処理を行います。プールは、クライアントがアクセスする Web アプリケーションのコンテンツをホストします。

◆注

*以下の手順は、バーチャルサーバの基本的な設定の概要のみを示したものです。バーチャルサーバ (SSL バーチャルサーバを含む)、およびその他のローカルトラフィックコンポーネントの詳細については、『**Configuration Guide for BIG-IP® Local Traffic Management**』を参照してください。*

バーチャルサーバおよびプールを作成するには

1. ナビゲーションペインの [Main] タブで、[**Local Traffic**] を展開して [**Virtual Servers**] をクリックします。
   [Virtual Server List] 画面が開きます。
2. [**Create**] ボタンをクリックします。
   [New Virtual Server] 画面が開きます。
3. [**Name**] ボックスに、バーチャルサーバの名前を入力します。
4. [**Destination Type] 設定**の [**Host**] ボタンをクリックし、[**Address**] ボックスに IP アドレスを入力します。
5. [**Service Port**] ボックスに **80 と入力するか**、リストから [**HTTP**] を選択します。
6. [**Configuration**] リストから、[**Advanced**] を選択します。
   画面が更新され、詳細設定オプションが表示されます。
7. [Configuration] 領域で、[**HTTP Profile**] リストから、作成した HTTP サービスプロファイルを選択します。
8. [**SNAT Pool**] 設定で、[**Auto Map**] を選択します。
9. [Resources] 領域で、[**HTTP Class Profiles**] 設定の [**Available**] リストから、作成した HTTP クラスプロファイルを選択し、移動ボタン（[<<]）をクリックして、クラスを [**Enabled**] リストに追加します。
10. [**Default Pool**] リストの隣の追加ボタン ([**+**]) をクリックします。
    [New Pool] 画面が開きます。
11. [**Name**] ボックスに、プールの名前を入力します。
12. [**Health Monitors**] で、[**Available**] リストから**ヘルスモニタを 1 つまたは複数選択し、**移動ボタン（[<<]）をクリックしてモニタを [**Available**] リストに追加します。
13. [Resources] 領域で、[**Load Balancing Method**] リストから負荷分散オプションを選択します。
14. [**Priority Group Activation**] 設定がデフォルトの [**Disabled**] であることを確認します。

15. [**New Members**] 設定で [**New Address**] を選択し、[**Address**] および[**Service Port**]ボックスにプールメンバのアドレスおよびポートを入力します。または、[**Node List**] を選択し、[**New Members**] リストに追加するノードを選択することもできます。
16. [**Add**] ボタンをクリックします。
17. [**Finished**] をクリックします。
    画面が更新され、[New Virtual Server] 画面が開きます。この画面の [**Default Pool**] リストには新しいプールが表示されています。
18. [**Finished**] をもう一度クリックします。
    設定が更新され、[Virtual Server] リスト画面が表示されます。この画面には、作成したバーチャルサーバが表示されています。

WebAccelerator 用のアプリケーションプロファイルの作成

*アプリケーションプロファイル*は、WebAccelerator がサイトの Web アプリケーションへの要求を適切に処理するために必要とする主要情報を提供します。アプリケーションプロファイルの作成は以下のタスクで構成されます。

- アプリケーションへのトラフィックを管理するための高速化ポリシーの選択
- ホストマップの計画と定義
- アプリケーションプロファイルの検証

高速化ポリシーの選択

アプリケーションプロファイルの作成プロセスを開始するには、最初に、アプリケーションに関連付ける高速化ポリシーを決定する必要があります。1 つの選択肢は、特定のアプリケーションパブリッシャーに関連付けられている事前定義済みの高速化ポリシーを選択するという方法です。

特定のアプリケーションパブリッシャー専用の高速化ポリシーの使用を望まない場合には、2 つの汎用事前定義済み高速化ポリシーのいずれかを使用できます。これらは 2 つとも、Java 2 Platform Enterprise Edition（J2EE）アプリケーションを使用するサイトのほとんどで良好に動作します。

- **Level 1 Delivery**
  この事前定義済み高速化ポリシーは、HTML バージョン 2.0 に準拠します。この高速化ポリシーの場合、WebAccelerator は以下のように動作します。
  - HTML ページに対するすべての要求を、コンテンツ発信元の Web サーバに送信します。
  - HTTP **Cache-Control** リクエストヘッダに含まれる no-cache 指示子を無視し、発信元 Web サーバから受信する cache response 指示子を使用します。

- **Level 2 Delivery**
  この事前定義済み高速化ポリシーは、HTML バージョン 3.0 以降に準拠します。この高速化ポリシーの場合、WebAccelerator は以下のように動作します。
  - HTML ページをキャッシュし、**0** のライフタイム設定を割り当てます。これは、WebAccelerator に対して、条件付き GET でそのコンテンツの以降の要求を行うことにより、最新のコンテンツを提供するように求めます。
  - Intelligent Browser Referencing 機能を documents および includes のみに使用します。
  - HTTP **Cache-Control** リクエストヘッダに含まれる no-cache 指示子を無視し、発信元 Web サーバから受信する cache response 指示子を使用します。

WebAccelerator では、アプリケーション固有および汎用配信の高速化ポリシー以外に、対向設置と呼ばれる設置方法に固有の高速化ポリシーも提供しています。オプションの対称展開を設定する場合は、このオプションを選択できます。このオプションの詳細については、『***Configuration Guide for the BIG-IP® WebAccelerator™ System***』を参照してください。

事前定義の高速化ポリシーを使用できない特殊なアプリケーションがある場合には、***ユーザ定義の高速化ポリシー*** を作成することにより、WebAccelerator の動作をカスタマイズできます。多くの場合、カスタマイズは、事前定義の高速化ポリシーをコピーし、これを必要に応じて変更することにより実施します。また、コンサルタントやベンダーなどが作成および認定し、暗号化した***署名付きの高速化ポリシー***をインポートするという選択肢もあります。

高速化ポリシー機能の詳細、ユーザ定義の高速化ポリシーの作成手順、署名付きの高速化ポリシーのインポート手順については、『***Policy Management Guide for the BIG-IP® WebAccelerator™ System***』を参照してください。

◆ ヒント

アプリケーションプロファイルの作成後、選択した高速化ポリシーはいつでも変更できます。

ホストマップの計画

WebAccelerator では HTTP リクエストを受信すると、リクエスト中のホストと***ホストマップ***上のホストを比較して、どのアプリケーションプロファイルを適用するかの決定を行います。システムがアプリケーションプロファイルに一致した後は、関連する高速化ポリシーを使用して要求を処理することができます。

ホストマップを作成する際、HTTP Host リクエストヘッダに示されるドメインを特定します。これらのドメインは、***requested host*** と呼ばれます。ホストマップに requested host 名を指定する場合、ワイルドカードとしてアスタリスク (*****) を使用し、その後にピリオドを続けることにより、ドメインの最初の文字を表すことができます。このワイルドカードは、複数のサブドメインを表すことができ、一度に複数のサブドメインを 1 つの発信元 Web サーバにマッピングすることができます。サイトに複数のサブドメインがある場合には、ワイルドカードを使用することにより、時間が節約されます。

◆ 注

*WebAccelerator は、マッピングされていないドメインの要求も管理できます。このようなリクエストはマップされていないリクエストと呼ばれます。詳細については、『**Configuration Guide for the BIG-IP® WebAccelerator™ System**』を参照してください。*

以下は、ワイルドカードを使用した有効な要求ホスト名の例を示します。

- ***.sales.siterequest.com** は、以下のようにマッピングします（宛先ホストはすべて同じ）。
  - **direct.sales.siterequest.com**
  - **marketing.sales.siterequest.com**
  - **marcom.marketing.sales.siterequest.com**
- ***siterequest.com** は、以下のようにマッピングします（宛先ホストはすべて同じ）。
  - **www.siterequest.com**
  - **engineering.siterequest.com**
  - **direct.sales.siterequest.com**
  - **marketing.sales.siterequest.com**
  - **marcom.marketing.sales.siterequest.com**
- ***.com** は、末尾が **.com** の受信ホストのすべてを 1 つの宛先ホストにマッピングします。
- ***.com** は、受信したすべての要求を 1 つの宛先ホストにマッピングします。

WebAccelerator が複数の要求ホスト名を 1 つの要求にマッピングできる場合、要求に最も近いホスト名が選択されます。以下のホスト名が定義されているとしましょう。

- **a.com**
- **www.a.com**
- ***.b.a.com**
- ***.a.com**

WebAccelerator がこれらの URL を含む要求を受信した場合、その要求は以下の要求ホストにマッピングされます。

- **www.a.com** に対する要求は、**www.a.com** にマッピングされ、***.a.com** にはマッピングされません。
- **a.com** に対する要求は、**a.com** にマッピングされます。
- **c.a.com** に対する要求および **b.a.com** に対する要求は、両方とも ***.a.com** にマッピングされます。
- **c.b.a.com** に対する要求は、***.b.a.com** にマッピングされます。

アプリケーションプロファイルを作成するには

1. ナビゲーションペインの [Main] タブで [**WebAccelerator**] を展開し、[**Applications**] をクリックします。
   新しいウィンドウに [Applications] 画面が表示されます。
2. [**Create**] ボタンをクリックします。
   [New Application] 画面が開きます。

3. [**Application Name**] ボックスに、アプリケーションの名前を入力します。
4. [**Description**] ボックスに説明を入力します（オプション）。
5. [**Central Policy**] リストから、関連するアプリケーションからの情報を要求する場合に WebAccelerator で使用する高速化ポリシーを選択します。オプションの対向設置を設定している場合には、**対向設置用**事前定義済み高速化ポリシーを選択することをお勧めします。このポリシーは、特に対向設置におけるコンテンツアセンブリの管理を目的としているためです。詳細については、『***Configuration Guide for the BIG-IP® WebAccelerator™ System***』を参照してください。
6. 対向設置を使用する場合は、[**Remote Policy**] リストから、リモート WebAccelerator 用の高速化ポリシーを選択します。**対向設置用**事前定義済み高速化ポリシーを選択することをお勧めします。対称展開を使用しない場合、リモートポリシーは選択しないでください。
7. 画面の下部の [Hosts] セクションで、[**Requested Host**] ボックスに有効なホスト名を入力します。
8. アプリケーションへのアクセス許可を与えるクライアントホストを追加する場合は、画面下部の [Hosts] セクションの [**Add Host**] ボタンを押します。
   画面が更新され、別の [**Requested Host**] ボックスが表示されます。ここに、追加のクライアントホストの名前を入力できます。
9. クライアントホストの追加が終了したら、[**Save**] ボタンをクリックします。

アプリケーションプロファイルの検証

アプリケーションプロファイルの作成後、WebAccelerator が正しくデータを送信し、発信元 Web サーバからデータを受信できることを検証する必要があります。

アプリケーションプロファイルを検証するには

1. WebAccelerator から独立しており、Web ブラウザを実行可能なマシン上で、**hosts** ファイルを開き、Web サイトアプリケーションのアクセスに使用したホスト名を追加します。このホスト名は、設定したバーチャルサーバの IP アドレスを指定するものであることが必要です。

   注 : Microsoft® Windows® 2000 および Windows® XP マシンの場合、hosts ファイルのパス名は C:\WINDOWS\system32\drivers\etc\hosts です。

   たとえば、**www.siterequest.com** ドメインの Web サイトをアクセスできる場合で、バーチャルサーバが IP アドレス **11.1.11.3** に配置されている場合、ブラウザを実行しているマシンの hosts ファイルに以下の行を追加します。

   ```
   11.1.11.3   www.siterequest.com
   ```

以降、**www.siterequest.com** の Web ブラウザマシンからのすべてのネットワークトラフィックは、バーチャルサーバに送信されます。

2. Web ブラウザマシンから、**www.siterequest.com** のページを要求します。

   ブラウザが発信元 Web サーバに直接アクセスしたなら受信していたはずのページが表示されます。ブラウザで要求がタイムアウトする場合、WebAccelerator が稼働していないか、WebAccelerator 上のポート **80** へのアクセスがファイアウォールでブロックされています。

3. **Access denied by intermediary error** を受信する場合、以下のタスクを実行します。

   - **hosts** ファイルが正しいことを検証します。
   - アプリケーションプロファイルのホストマップが正しいことを検証します。
   - 要求で使用したドメインがホストマップの要求ホストに一致していることを検証します。

4. ホストマッピングを確認した後、変更や追加を行ったエントリのすべてを削除します。

Protocol Security Module 設定での HTTP セキュリティプロファイルの作成

Protocol Security Moduleでは、***HTTP セキュリティプロファイル***によって、Security Enforcer で実施される HTTP セキュリティチェックを指定します。また、WebAccelerator アプリケーションプロファイルをセキュリティプロファイルに関連付けます。プロトコルセキュリティプロファイルの詳細については、『***Configuration Guide for BIG-IP® Protocol Security Module***』を参照してください。このドキュメントは、**https://support.f5.com** から入手できます。

◆ 重要

*以下のタスクは、セキュリティプロファイルのログファイルに対するリモートロギング設定のセットアップがすでに完了していることを前提にしています。リモートロギングおよび Protocol Security Module の詳細については、『**Configuration Guide for BIG-IP® Protocol Security Module**』を参照してください。*

HTTP トラフィックのセキュリティプロファイルを作成するには

1. ナビゲーションペインの [Main] タブで、[**Protocol Security**] を展開して [**Security Profiles**] をクリックします。
   [HTTP Security Profiles] 画面が新しいブラウザセッションに表示されます。
2. [HTTP Security Profiles]領域の上の[**Create**]ボタンを押します。
   [New Security Profile] 画面が開きます。
3. [Profile Properties] 領域で、[**Profile Name**] ボックスに、プロファイルの固有の名前を入力します。
4. [**Remote Logging**] 設定で、チェックボックスをオンにし、このセキュリティプロファイルのリモートロギングを有効にします。
5. [Defense Configuration] 領域では、タブをクリックし、必要に応じて設定を変更することにより、セキュリティプロファイルに関するブロックポリシー設定を更新することができます。違反時の [**Alarm**] または [**Block**] のいずれのチェックボックスをオンにしていない場合、対応するセキュリティチェックは実施されません。
   - セキュリティプロファイル違反を引き起こす要求をログに記録するには、[**Alarm**] チェックボックスをオンにします。
   - セキュリティプロファイル違反を引き起こす要求をブロックするには、[**Block**] チェックボックスをオンにします。
   - 両方の動作を実行するには、[**Alarm**] と [**Block**] の両方のチェックボックスをオンにします。

6. [Blocking Page] タブをクリックして、ブロック応答ページを設定します。違反時の [Block] フラグを有効化している場合、違反クライアントはアプリケーションに接続されず、その代わりにブロック応答ページが違反クライアントに送信されます。
7. [WebAccelerator] タブをクリックします。このタブで、WebAcceleratorアプリケーションプロファイルをHTTPセキュリティプロファイルに関連付けます。
8. [**WebAccelerator Cache Clear Settings**]オプションの[**Available WA Applications**]リストから、WebAcceleratorアプリケーションプロファイルを選択し、移動ボタン（<<）をクリックしてプロファイルを [**Assigned WA Applications**] リストに追加します。
9. [**Create**] をクリックします。
画面が更新され、新しいセキュリティプロファイルがリストに表示されます。

用語集

ARP（Address Resolution Protocol）

ARP は業界標準のプロトコルで、ホストの MAC（Media Access Control）アドレスをその IP アドレスに基づいて判定します。

BIND（Berkely Internet Name Domain）

BIND は、DNS（Domain Name System）の最も一般的な実装です。BIND によって、BIG-IP は IP アドレスに一致するドメイン名を取得できます。詳細については、**http://www.isc.org/products/BIND** を参照してください。

Certificate Revocation List Distribution Point (CRLDP)

「*CRLDP （Certificate Revocation List Distribution Point）*」を参照してください。

Cookie パーシステンス

Cookie パーシステンスは、パーシステンスのモードの 1 つで、BIG-IP がパーシステンスコネクション情報を Cookie に保存できます。

CRL（証明書失効リスト）

CRL は、認証するシステムが、要求側のシステムが認証用に提示した SSL 証明書が無効になっていないか確認するためのリストです。

CRLDP（Certificate Revocation List Distribution Point）

CRLDPは業界標準のプロトコルで、ネットワーク上のデバイスのSSL証明書失効を管理します。

CRLDP 認証モジュール

CRLDP 認証モジュールは、ユーザ作成のモジュールで、BIG-IP 上で実装してCRLDPプロトコルを使用してクライアントトラフィックを認証します。ネットワーク上のクライアント SSL 証明書の無効状態の管理を目的とします。

external VLAN

external VLAN は、BIG-IP のデフォルト VLAN のうちのひとつです。基本設定では、この VLAN の管理ポートはロックダウンが設定されています。通常の設定では、これは外部クライアントが内部サーバへの接続を要求する VLAN になります。

ICMP（Internet Control Message Protocol）

ICMP は、宛先アドレスへのルート情報の判定に使用される、インターネット通信プロトコルです。

internal VLAN

internal VLAN は、BIG-IP のデフォルト VLAN です。基本設定では、この VLAN の管理ポートは開いています。通常の設定では、これは内部サーバからの接続を処理するネットワークインターフェイスになります。

iRule

iRule はユーザ作成のスクリプトで、BIG-IP を通過する接続の動作を制御します。iRules™ は F5 ネットワークスの機能で、特定の接続をデフォルト以外のロードバランシングプールに振り分ける場合によく使用されます。ただし iRule では、安全なネットワークアドレス変換の実装やセッションパーシステンスの実現など、その他のタスクも実行できます。

Kerberos プロトコル

Kerberos プロトコルはネットワーク認証プロトコルで、安全でないネットワークを介して通信を行う個人が、安全な方法でその身元を他方に証明できるようにします。主にクライアント - サーバモデルでの使用を目的としていて、相互認証により、ユーザとサーバの両方がそれぞれの身元を確認します。

LACP（Link Aggregation Control Protocol）

LACP はトランク内のリンクを集約する業界標準のプロトコルで、帯域幅を増加させてリンクフェイルオーバーを提供します。

LDAP（Lightweight Directory Access Protocol）

LDAP は、電子メールプログラムがサーバから宛先情報を検索する際に使用するインターネットプロトコルです。

LDAP 認証モジュール

LDAP 認証モジュールは、BIG-IP 上に実装するユーザ作成のモジュールで、リモート LDAP サーバを使用してクライアントトラフィックを認証します。

LDAP クライアント証明書 SSL 認証モジュール

LDAP クライアント証明書 SSL 認証モジュールは、BIG-IP 上に実装するユーザ作成のモジュールで、SSL クライアント証明書とリモート LDAP サーバを使用してクライアントトラフィックを認証します。

Link Aggregation Control Protocol（LACP）

「*LACP（Link Aggregation Control Protocol）*」を参照してください。

MAC（Media Acces Control）

MAC は、ワークステーションが転送メディアへアクセスする方法を定義するプロトコルで、LAN に関して一般的に使用されています。IEEE LAN では、MAC 層はデータリンク層プロトコルの下位サブレイヤです。

NAT（Network Address Translation：ネットワークアドレス変換）

NAT は、BIG-IP が管理する特定のノードを特定する、外部ネットワークに対するエイリアス IP アドレスです。

OCSP（Online Certificate Status Protocol）

OCSP は、認証システムがデジタル署名された SSL 証明書の無効状態のチェックに使用するプロトコルです。OCSP は、CRL（証明書失効リスト）の代替手段として使用できます。「*CRL（証明書失効リスト）*」も参照してください。

OCSP 認証モジュール

OCSP 認証モジュールは、BIG-IP 上に実装するユーザ作成のモジュールで、リモート OCSP レスポンダを使用してクライアントトラフィックを認証します。OCSP 認証モジュールの目的は、クライアント SSL 証明書の無効状態をチェックすることです。

OCSP レスポンダ

OCSP レスポンダは、BIG-IP などの認証サーバに SSL 証明書失効状態を伝える場合に使用される、外部サーバです。

OCSP レスポンダオブジェクト

レスポンダオブジェクトは、BIG-IP 上のソフトウェアアプリケーションで、OCSP レスポンダと通信して、クライアントまたはサーバ SSL 証明書の失効状態をチェックします。

PAM（Pluggable Authentication Module）

PAM モジュールは、サーバアプリケーションがクライアントトラフィックの認証に使用するソフトウェアモジュールです。PAM モジュールはモジュラー設計されているため、サーバアプリケーションへの認証メカニズムの追加、置換、削除を、アプリケーションに与える影響を最小限にして実行できます。PAM モジュールの例として、リモート LDAP（Lightweight Directory Access Protocol）サーバを使用してクライアントトラフィックを認証するアプリケーションがあります。「*LDAP（Lightweight Directory Access Protocol）*」も参照してください。

RADIUS（Remote Authentication Dial-in Service）

RADIUS は、リモートユーザ認証とアカウンティングを実行するサーバです。主にインターネットサービスプロバイダが利用しますが、ワークステーションで一元化した認証および(または)アカウンティングサービスを必要とするあらゆるネットワークで使用することもできます。

RADIUS 認証モジュール

RADIUS 認証モジュールは、ユーザ作成のモジュールで、BIG-IP 上に実装し、リモート RADIUS サーバを使用してクライアントトラフィックを認証します。

RAM キャッシュ

RAM キャッシュは、BIG-IP の RAM に保存される HTTP オブジェクトのキャッシュで、以降の接続で再利用され、バックエンドサーバの負荷を低減できます。

SNAT（セキュアネットワークアドレス変換）

SNAT は、BIG-IP で設定できる機能です。SNAT は、ネットワーク上のホストに接続する場合に、1 つ以上のノードが送信元 IP アドレスとして使用できる、転送可能なエイリアス IP アドレスを定義します。

SNMP（Simple Network Management Protocol）

SNMP はインターネット標準のプロトコルで、STD15 RFC 1157 で定義され、IP ネットワーク上のノード管理のために開発されました。

SSH

SSH はセキュアリモートログインと、非セキュアネットワークでセキュアネットワークサービスを実現するためのプロトコルです。

SSL（Secure Sockets Layer）

SSL はネットワーク通信プロトコルで、データを安全に転送する方法として公開鍵テクノロジを使用しています。

SSL プロファイル

SSL プロファイルは設定ツールで、クライアントおよびサーバから SSL 接続を終端および開始するために使用します。

TACACS（Terminal Access Controller Access Control System）

TACACS は UNIX システムでよく使用される、古いタイプの認証プロトコルです。TACACS では、リモートアクセスサーバはユーザのログインパスワードを認証サーバに転送できます。

TACACS+

TACACS+ は、それ以前の TACACS プロトコルを置き換えるために設計された認証メカニズムです。この 2 つのプロトコルに類似点はほとんどなく、したがって互換性はありません。

TACACS+ 認証モジュール

TACACS+ 認証モジュールは、ユーザ作成のモジュールで、BIG-IP 上に実装し、リモート TACACS+ サーバを使用してクライアントトラフィックを認証します。

TMM（Traffic Management Microkernel）サービス

TMM サービスは、BIG-IP で実行されるプロセスで、BIG-IP 上のトラフィック管理の大半を実行します。

VLAN（仮想ローカルエリアネットワーク）

VLAN は、ネットワークデバイスに接続されたインターフェイスを、論理的にグループ化したものです。VLAN を使用して、別のネットワークセグメントにあるデバイスを、論理的にグループ化できます。VLAN 内のデバイスは、レイヤ 2 ネットワーキングを使用して通信し、ブロードキャストドメインを定義します。

VLAN グループ

VLAN グループは、2 つ以上の VLAN を 1 つの VLAN グループにまとめたものです。VLAN グループの主な使用方法は、送信元と宛先ホストの両方が同じネットワーク上にある場合、トラフィックを正常に転送することです。

VLAN 名

VLAN 名は、VLAN を識別するために使用するシンボル名です。たとえば、**marketing** または **development** という名の VLAN を設定できます。「*VLAN (仮想ローカルエリアネットワーク)*」も参照してください。

VLAN タグ

VLAN タグは IEEE 標準で、フレームのヘッダに挿入された識別番号で、宛先デバイスが属する VLAN を示します。VLAN タグは、1 つのインターフェイスが複数の VLAN にトラフィックを転送する場合に使用されます。

アクティブユニット

アクティブユニットとは、冗長システムで現在コネクションのロードバランスを実行しているシステムです。冗長システムのアクティブユニットに障害が起きた場合に、スタンバイユニットに制御が引き継がれ、コネクションのロードバランスを実行します。「*冗長システム*」も参照してください。

インターフェイス

BIG-IP の物理ポートは、インターフェイスと呼ばれます。

親プロファイル

親プロファイルは、その値を他のプロファイルに伝播できるプロファイルです。親プロファイルは、デフォルトプロファイルまたはカスタムプロファイルのどちらでも可能です。「*プロファイル*」も参照してください。

カスタムプロファイル

カスタムプロファイルは、ユーザが作成するプロファイルです。カスタムプロファイルは、指定した親プロファイルのデフォルト設定を継承できます。「*親プロファイル*」、「*プロファイル*」も参照してください。

仮想アドレス

仮想アドレスは、BIG-IP で管理される 1 つ以上のバーチャルサーバに関連付けられた IP アドレスです。「*バーチャルサーバ*」も参照してください。

仮想ポート

仮想ポートは、BIG-IP で管理される 1 つ以上のバーチャルサーバに関連付けられたポート番号またはサービス名です。仮想ポート番号は、クライアントプログラムが接続する先の TCP または UDP ポート番号と同じである必要があります。

管理インターフェイス

管理インターフェイスは、BIG-IP の特殊なポートで、管理トラフィックの管理に使用されます。**MGMT** と呼ばれ、管理インターフェイスは、ロードバランシングされるトラフィックなどのユーザアプリケーショントラフィックは転送しません。

ゲートウェイプール

ゲートウェイプールはルータのプールで、トラフィックを転送するために作成します。ゲートウェイプールを作成したら、TMM ルーティングテーブルエントリ内でプールをゲートウェイとして指定できます。

構成オブジェクト

構成オブジェクトはユーザが作成したオブジェクトで、BIG-IP はこれを使用して PAM 認証モジュールを実装します。作成する認証モジュールの各タイプに対して、それぞれ 1 つのタイプの構成オブジェクトがあります。「*PAM（Pluggable Authentication Module）*」も参照してください。

コネクションパーシステンス

コネクションパーシステンスは、ハンドシェイクを省くためにネットワーク接続を意図的に開いたままにする、最適化テクニックです。

サービス

TCP、UDP、HTTP、FTP などのサービスのことです。

冗長システム

冗長システムは、フェイルオーバー用に設定された 2 台のユニットです。冗長システムでは 2 つのユニットがあり、1 つはアクティブユニットとして実行され、もう 1 つはスタンバイユニットとして実行されます。アクティブユニットに障害が発生すると、スタンバイユニットが処理を引き継いで接続要求を管理します。

承認

承認は、ログオンしたユーザに付与するシステムリソースへのアクセス権限のレベルを特定するプロセスです。

証明書

証明書は、信頼された認証局が署名し、SSL ネットワークトラフィックに認証手段として使用される、オンライン認証情報です。

証明書失効リスト（CRL）

「*CRL（証明書失効リスト）*」を参照してください。

シンプルパーシステンス

「*送信元 IP アドレスパーシステンス*」を参照してください。

スタンバイユニット

冗長システムのスタンバイユニットは、アクティブユニットで障害が発生したときにいつでもアクティブユニットに交代できるユニットです。

スパニングツリー

スパニングツリーは、ネットワーク上のレイヤ 2 デバイスの論理的ツリー構造で、スパニングツリープロトコルアルゴリズムによって作成され、ネットワークループの解決に使用されます。

セキュアネットワークアドレス変換（SNAT）

「*SNAT（セキュアネットワークアドレス変換）*」を参照してください。

セッションパーシステンス

同じクライアントから受信した一連の関連する接続で、同じセッション ID を持っています。パーシステンスを有効にすると、BIG-IP は同じセッション ID を持つすべての接続を同じノードに送信します。接続にロードバランシングは実行されません セッションパーシステンスと「*コネクションパーシステンス*」は、別のものです。

設定ユーティリティ

設定ユーティリティは、ブラウザベースのアプリケーションで、BIG-IP の設定に使用します。

セットアップユーティリティ

セットアップユーティリティを使用して、初期システム設定を処理できます。セットアップユーティリティは、設定ユーティリティのスタートページから実行できます。

セルフ IP アドレス

セルフ IP アドレスは、BIG-IP が持つ IP アドレスで、内部および外部 VLAN へのアクセスに使用できます。

送信元 IP アドレスパーシステンス

シンプルパーシステンスとも呼ばれます。送信元 IP アドレスパーシステンスは、TCP および UDP プロトコルをサポートし、パケットの送信元IPアドレスのみに基づいて同じサーバにセッション要求をダイレクトします。

タグ付きインターフェイス

タグ付きインターフェイスは、VLAN に割り当てられるインターフェイスで、BIG-IP はそのインターフェイスを通過したフレームのヘッダに VLAN タグを追加します。タグ付きインターフェイスは、複数の VLAN に 1 つのインターフェイスを割り当てる場合に使用します。「*VLAN（仮想ローカルエリアネットワーク）*」も参照してください。

チェーン

チェーンは一連のフィルタ基準で、IP アドレスへのアクセスを制限します。チェーン内での基準の順序によって、一般的な基準を先に適用し、詳細な基準をチェーンの最後に適用するなど、フィルタの適用方法を規定します。

定義済みモニタ

定義済みモニタは、BIG-IP が提供するヘルスモニタまたはパフォーマンスモニタです。定義済モニタはそのまま使用できますが、変更したり削除したりすることはできません。「*モニタ*」も参照してください。

デフォルト VLAN

BIG-IP では、2 つのデフォルト VLAN が設定されており、それぞれひとつのインターフェイスに割り当てられています。デフォルト VLAN には、**internal**（内部）と **external**（外部）があります。「*VLAN（仮想ローカルエリアネットワーク）*」も参照してください。

デフォルトプロファイル

デフォルトプロファイルは、BIG-IP がデフォルト設定値で提供するプロファイルです。デフォルトプロファイルをそのまま使用することも、変更することもできます。デフォルトプロファイルは、カスタムプロファイルを作成するときの親ファイルに指定することもできます。デフォルトプロファイルの作成や削除はできません。「*プロファイル*」、「*カスタムプロファイル*」も参照してください。

デフォルトルート

デフォルトルートは、ルーティングテーブルで指定されたルートに、宛先アドレスや転送されるパケットのネットワークに一致するものがない場合にシステムが使用するルートです。

デフォルトワイルドカードバーチャルサーバ

デフォルトワイルドカードバーチャルサーバは、IP アドレスとポート番号として、**0.0.0.0:0** または ***:*** または **"any":"any"** が設定されています。このバーチャルサーバは、設定で定義されたその他のバーチャルサーバに一致しないすべてのトラフィックを受信します。

ドメイン名

ドメイン名は、1 つ以上の IP アドレスに関連付けられた一意の名前です。ドメイン名は、URL で使用して特定の Web ページを指定します。たとえば、**http://www.siterequest.com/index.html** という URL では、ドメイン名は **siterequest.com** です。

トランク

トランクは、2つ以上のインターフェイスとケーブルを組み合わせて、1 つのリンクとして構成したものです。

トランスペアレントノード

トランスペアレントノードは、BIG-IP を含め、他のネットワークデバイスからはルータとして認識されます。

認証

認証は、ユーザが BIG-IP にログオンしようとするときに、ユーザの真正性を検証するプロセスです。

認証 iRule

認証 iRule は、BIG-IP 付属またはユーザ作成の iRule で、BIG-IP で PAM 認証モジュールを実装するために必要です。「*iRule*」、「*PAM (Pluggable Authentication Module)*」も参照してください。

認証局（CA）

認証局は、外部の信頼された機関で、SSL ネットワークトラフィックの認証を取得するための資格情報として使用する署名済みデジタル証明書を、要求したコンピュータシステムに発行します。

認証プロファイル

認証プロファイルは設定ツールで、PAM 認証モジュールを実装するときに使用します。認証プロファイルで実装できる認証モジュールのタイプは、LDAP、RADIUS、TACACS+、SSL クライアント証明書 LDAP、および OCSP です。「*PAM (Pluggable Authentication Module)*」も参照してください。

認証モジュール

認証モジュールは、ユーザが作成した PAM モジュールで、クライアントトラフィックの認証または承認を実行します。「*PAM（Pluggable Authentication Module）*」も参照してください。

ノード

ノードは、BIG-IP の論理オブジェクトで、ネットワーク上の物理リソースの IP アドレスを特定します。ノードは、プールメンバとモニタに直接関連付けられます。「*プールメンバ*」、「*モニタ*」も参照してください。

パーシステンスプロファイル

パーシステンスプロファイルは、特定のタイプのセッションパーシステンスを実装する設定ツールです。パーシステンスプロファイルタイプの例として、Cookie パーシステンスプロファイルがあります。

バーチャルサーバ

バーチャルサーバは、BIG-IP や他のホストサーバによって管理されているコンテンツサイトに関連付けられた仮想アドレスと仮想ポートの特定の組み合わせを指します。

パーティション

パーティションは、定義されたBIG-IPシステムオブジェクトのセットを含む、ユーザにより作成される論理コンテナです。パーティションを使用して、BIG-IP へのユーザアクセスを制御します。「*ユーザロール*」も参照してください。

パフォーマンスモニタ

パフォーマンスモニタは、統計情報を収集してターゲットデバイスの状態を確認します。

プール

プールは、プールメンバの論理グループです。BIG-IP は、プール設定時に選択したロードバランシング方式とパーシステンス方式に従って、プールメンバに対する要求をロードバランスします。「*ノード*」、「*プールメンバ*」も参照してください。

プールメンバ

プールメンバは、ロードバランシングプールのメンバの 1 つです。プールメンバ名は、ノード IP アドレスとサービス番号を示します。「*ノード*」も参照してください。

フェイルオーバー

フェイルオーバーは、アクティブユニット上でソフトウェア障害またはハードウェア障害が検出された場合に、冗長システムのスタンバイユニットが処理を引き継ぐプロセスです。

フォワーディングバーチャルサーバ

フォワーディングバーチャルサーバは、ロードバランス対象となるプールメンバを持たないバーチャルサーバです。バーチャルサーバは、クライアント要求で指定されている宛先 IP アドレスにパケットを直接転送するだけです。「*バーチャルサーバ*」も参照してください。

フローティングセルフ IP アドレス

フローティングセルフ IP アドレスは、VLAN の追加セルフ IP アドレスで、BIG-IP 冗長システムの両方のユニットで共有されるアドレスです。

プロトコルプロファイル

プロトコルプロファイルは、FastL4、TCP、UDP トラフィックの動作を制御するために作成するプロファイルです。

プロファイル

プロファイルは、ネットワークトラフィックの動作を定義する設定を含む、設定ツールです。BIG-IP には、FastL4、HTTP、TCP、FTP、SSL トラフィックを管理し、パーシステンスおよびアプリケーション認証を実装するプロファイルがあります。

プロファイル設定

プロファイル設定は、プロファイル内の設定属性で、値が関連付けられています。プロファイル設定を行って、BIG-IP がトラフィックを管理する方法をカスタマイズできます。

プロファイルタイプ

プロファイルタイプは、特定の目的に使用できるプロファイルのカテゴリです。プロファイルタイプの 1 つに HTTP プロファイルがありますが、これはHTTPネットワークトラフィックの管理用に設定します。

ヘルスモニタ

ヘルスモニタは、ノードが **up** で指定されたサービスを実行しているか確認します。ノードがこのチェックに合格しないと、**down** と判定されます。チェックするサービスごとに、異なるモニタがあります。

ポート

ポートは、ホストがサポートする特定のサービスに関連付けられた番号で表されます。ポート番号と対応するサービスの一覧については、「*サービス*」および「*ポート*」の項目を参照してください。

ポート固有のワイルドカードバーチャルサーバ

ポート固有のワイルドカードバーチャルサーバは、**0** 以外のポート番号を使用するワイルドカードバーチャルサーバです。「*ワイルドカードバーチャルサーバ*」も参照してください。

モニタ

BIG-IP はモニタを使用して、ノードが **up** か **down** かを判定します。モニタには複数の種類があり、さまざまな手法を使用してサーバまたはサービスの状態を判定します。モニタをノード、プール、および個々のプールメンバに関連付けることができます。「*ノード*」、「*プール*」、「*プールメンバ*」も参照してください。

モニタインスタンス

モニタインスタンスは、ヘルスモニタがプールメンバまたはノードに関連付けられるときに作成します。ヘルスチェックを実際に実行するのはモニタインスタンスで、モニタではありません。

ユーザロール

ユーザロールは、BIG-IP ユーザアカウントに割り当てる、アクセス権限のタイプとレベルです。ユーザロールを割り当てることで、BIG-IP のシステム管理者が BIG-IP の設定を表示して変更できる範囲を制御できます。

リンクアグリゲーション

リンクアグリゲーションは、複数のリンクを結合し、1 つのリンクとして処理することで帯域幅を増加させるプロセスです。リンクアグリゲーションは、トランクを作成すると発生します。「*trunk*」、「*LACP（Link Aggregation Control Protocol）*」も参照してください。

ルータ

ルータは、レイヤ 3 ネットワーキングデバイスです。ネットワークで VLAN が定義されていない場合、ルータがブロードキャストドメインを定義します。

レイヤ 1 からレイヤ 7

レイヤ 1 からレイヤ 7 は、OSI（Open System Interconnection）モデルの 7 層を示します。つまり、レイヤ 2 はデータリンク層、レイヤ 3 は IP 層、レイヤ 4 はトランスポート層（TCP および UDP）を表します。レイヤ7はアプリケーション層で、HTTPおよびSSLなどのトラフィックを処理します。

レートクラス

レートフィルタは、設定ユーティリティまたはコマンドラインユーティリティから作成できます。レートクラスをレートフィルタに割り当てると、レートクラスは、レートフィルタで許可されるトラフィックの量を判定します。「*レートシェーピング*」も参照してください。

レートシェーピング

レートシェーピングは、拡張 IP フィルタの一種です。レートシェーピングは同じ IP フィルタ方式を使用しますが、レートクラスを適用して、許可されたネットワークトラフィックの量を判定します。「*レートクラス*」も参照してください。

レスポンダオブジェクト

「*OCSP レスポンダオブジェクト*」を参照してください。

ローカルトラフィック管理

ローカルトラフィック管理は、イントラネットなどのローカルエリアネットワーク（LAN）から送受信されるネットワークトラフィックを管理するプロセスです。BIG-IP® LTM を使用して、ローカルトラフィックを管理できます。

ロードバランシングバーチャルサーバ

ロードバランシングバーチャルサーバは、クライアントトラフィックをロードバランシングプールにダイレクトするバーチャルサーバで、バーチャルサーバの基本タイプです。「*バーチャルサーバ*」も参照してください。

ロードバランシングプール

「*プール*」を参照してください。

ロードバランシング方式

接続をロードバランシングプールに分散させる方法を決定する特定の方式です。

ワイルドカードバーチャルサーバ

ワイルドカードバーチャルサーバは、IP アドレスとして、0.0.0.0、*、または "any" を使用するバーチャルサーバです。ワイルドカードバーチャルサーバは、ローカルネットワークの外部の宛先への接続要求を受理します。ワイルドバーチャルサーバは、透過ノードモードの設定の場合にのみ使用できます。

索引

記号

/config/bigip.conf ファイル 27-3
/etc/radvd.conf ファイル 20-1

数字

1IP ネットワークトポロジ 17-6

A

ACK パケット 2-2, 2-6
Active Directory リモート認証 24-2
adaptive 方式 28-2
Administrator ロール
　オブジェクト管理 23-4
Administrator ロールアクセス 23-2
admin アカウント 23-2
Application Security Manager
　HTTP クラスプロファイル 29-3
ARP プロトコル 2-5
authentication
　リモートユーザアカウント 24-1

B

Back Orifice 攻撃 22-12
BIG-IP
　スイッチの交換 4-2
　設定、同じネットワーク 4-3
　追加、ネットワーク 4-1
BIG-IP システムオブジェクト 23-1
BIG-IP の迂回 2-1
bigpipe -? コマンド 24-8

C

Certificate Revocation List Distribution Point プロトコル
　CRLDP 認証モジュールを参照
Client SSL プロファイル
　作成 11-3, 12-3
　定義 11-1, 12-1
　トンネリング 28-9
　割り当て 11-6, 12-7
Common 23-2
Common パーティション
　説明 23-2
Cookie 22-8
Cookie パーシステンス 9-1
Cookie パーシステンスプロファイル 9-2
CRLDP 構成オブジェクト
　定義 25-21
CRLDP サーバオブジェクト
　定義 25-20
CRLDP 認証モジュール
　定義 25-20
CRLDP プロファイルタイプ
　定義 25-21
CRLDP レスポンダオブジェクト
　定義 25-20

D

deflate 方式 28-2
Deployment Wizard
　概要 29-13
　起動 29-13
　展開シナリオ 29-13
DNS サーバ
　設定 30-2

F

FastL4 プロファイル
　nPath ルーティング 2-2
　作成 2-2, 2-3
　割り当て 2-4
FIN パケット 2-2
FTP トラフィック 14-1
FTP バーチャルサーバ
　作成 14-4, 15-5
FTP プール
　作成 14-3, 15-3
　割り当て 14-4
FTP プロファイル
　定義 14-1
　割り当て 14-4
FTP モニタ 14-2, 15-2

G

Guest ロールのタスク 23-3

H

hbigpipe シェル
　ユーザロール 23-2
hosts ファイルの検証 29-11
HTML ページ
　キャッシュ 29-7
HTTP RAM キャッシュ
　RAM キャッシュを参照
HTTPS トラフィック 11-6
HTTPS バーチャルサーバ
　作成 11-6, 12-7
HTTPS プール
　作成 11-5, 12-6
　割り当て 11-6, 12-7
HTTP 圧縮作業 10-1
HTTP クラスプロファイル
　Application Security Manager 29-3
　WebAccelerator 29-3
　作成 29-3, 30-3
　重要な考慮事項 29-4
　設定オプション 29-4
HTTP サービスプロファイル
　作成 30-4
HTTP セキュリティプロファイル
　説明 30-12
HTTP 接続 9-3
HTTP トラフィック
　制御、Cookie パーシステンス 9-1
　制御、圧縮 10-1
　制御、送信元アドレスのパーシステンス 8-1

HTTP バーチャルサーバ
作成、Cookie パーシステンス 9-4
作成、圧縮 10-3
作成、送信元アドレスのパーシステンス 8-3
HTTP プール
作成、Cookie パーシステンス 9-3
作成、送信元アドレスのパーシステンス 8-2
割り当て、RAM キャッシュ 13-3
割り当て、圧縮 10-3
割り当て、送信元アドレスのパーシステンス 8-3
HTTP プロファイル
作成、LDAP 認証 25-15
作成、RAM キャッシュ 13-2
作成、圧縮 10-2, 12-4
説明 8-1
定義 9-1
HTTP ヘッダ 13-1
HTTP メソッド 13-1

I

ICMP フラッド 22-9
Intelligent Browser Referencing 機能 29-7
IPv6 ノード 20-2
IP アドレス
nPath ルーティング 2-5
VLAN から削除 17-7
ループバックインターフェイス 2-5
割り当て 21-1
IP アドレス変換 2-1
IP ネットワーク
変更 4-1
IP ネットワークトポロジ
単一インターフェイス 4-1, 16-1
IP パケット
認識、クライアント 16-5
ルーティング、不正 2-5
iRule
圧縮 10-1
iSession コンテキスト 28-8, 28-11
iSession プロファイル
作成 28-5
トンネリング 28-6, 28-9
ポート透過性 28-11
iSession ポート 3701 28-11

J

J2EE
標準配信の高速化ポリシー 29-7, 30-7
Java 2 Platform Enterprise Edition
J2EE を参照

L

L2 フォワーディング 4-1
LACP プロトコル 17-3
Land 攻撃 22-10
LDAP 構成オブジェクト
定義 25-2
LDAP プロファイルタイプ
定義 25-5
LDAP リモート認証 24-2
Lempel-Ziv-Oberhumer 方式 28-2
Level 1 Delivery 高速化ポリシー 30-7, 29-7
Level 2 Delivery 高速化ポリシー 29-7
lzo 方式 28-2

M

Manager ロールアクセス 23-2
Manager ロールのタスク 23-3
MS Loopback インターフェイス 2-5

N

NAS-Identifier 文字列 25-8
Network Time Protocol
NTP を参照。NTP
定義
nPath ルーティング 2-1, 2-5
nPath ルーティング作業 2-2
NTP
サーバの設定 29-6
NTP プロトコル
システムクロックの同期 30-2
Network Time Protocol Server。NTP を参照。

O

OCSP 認証モジュール
SSL OCSP 認証モジュールを参照
OCSP レスポンダオブジェクト
作成 25-17
Online Certificate Status Protocol
SSL OCSP 認証モジュールを参照
Operator ロールのタスク 23-3
Other External Users アカウント 24-6

P

Ping of Death 攻撃 22-10
Platform Guide 1-2

R

RADIUS secret 25-7
RADIUS 構成オブジェクト
作成 25-8
指定、プロファイル 25-9
RADIUS 構成の概要 25-7
RADIUS サーバ
トラフィック認証 25-7
認証 25-7
RADIUS サーバオブジェクト
作成 25-7
指定、構成オブジェクト 25-8
RADIUS サーバ構成 27-2
RADIUS 認証プロファイル
割り当て 25-9
RADIUS 認証モジュール
実装 25-7

RADIUS プロファイル
作成 25-9
RADIUS ベースの認証
設定 24-4
RADIUS ユーザ認証
設定 24-4
radvd サービス 20-1
RAM キャッシュ
http-acceleration プロファイル 29-5
WebAccelerator 29-5
定義 13-1
RAM キャッシュバーチャルサーバ 13-3
RAM キャッシュ機能
トンネリング 28-7
RAM キャッシュの準拠性 13-1
Read アクセス 23-2
remoterole コマンド
目的 24-1, 24-6, 24-7
remoterole コマンドの構文 24-7
requested host
定義 30-8
RTO 2-6

S

SCF
作成 24-11
目的 24-11
SNAT
作成 18-2
SNAT 自動マップ
VLAN 7-5
概要 7-1
SNAT 送信元変換 16-1
SSL OCSP 構成オブジェクト
作成 25-18
SSL OCSP 認証モジュール
定義 25-17
SSL OCSP プロファイルタイプ
定義 25-18
SSL OCSP レスポンダオブジェクト
作成 25-17
SSL キーと証明書
インストール 12-1
作成 11-2, 12-2
SSL クライアント証明書 LDAP 構成オブジェクト
作成 25-14
SSL クライアント証明書 LDAP プロファイル
作成 25-15
SSL 証明書
インポート 24-2
SSL トラフィックの認証 24-2
SSL ハンドシェイク
HTTPS 11-1, 11-2, 11-6
圧縮 12-1, 12-2
SSL プロファイル
Client SSL プロファイルを参照
Sub 7 攻撃 22-11
SYN Cookie 22-8, 22-9
SYN チェック機能、有効化 22-9
SYN パケット 2-2, 2-6
SYN フラッド 22-8

T

TACACS+ 構成オブジェクト
定義 25-11
TACACS+ 構成の概要 25-11
TACACS+ プロファイル
作成 25-12
tcpdump ユーティリティ 18-1
TCP 最適化プロファイル
トンネリング 28-6, 28-9
TCP 接続 22-8
TCP タイマ 2-6
TCP トラフィック
nPath ルーティング 2-2, 2-6
Teardrop 攻撃 22-11

U

UDP タイマ 2-6
UDP トラフィック
nPath ルーティング 2-6
UDP フラグメント攻撃 22-10
UDP フラッド 22-9
URI
包含と除外 10-1

V

VLAN
削除、セルフ IP アドレス 4-3, 4-4
使用、リンクアグリゲーション 17-1
タグ付きインターフェイス 5-2
パーティション 23-2
VLAN グループ
作成 4-4, 17-7
VLAN タグ
作成 5-2, 17-3

W

WebAccelerator
HTTP クラスプロファイル 29-3
NTP プロトコル 30-2
Protocol Security Manager とともに実行 30-3
アプリケーションプロファイル 30-1
セキュリティプロファイル 30-1
WebAccelerator アプリケーションプロファイル
プロトコルセキュリティ 30-12
Web アプリケーション
ホストされるコンテンツ 29-4, 30-5
Web アプリケーションコンテンツ
ホスト 29-4, 30-5
Web サーバアレイ 3-1
Web サーバプール
作成 4-5
[Welcome] 画面 1-5
WinNuke 攻撃 22-11

あ

アイドルタイムアウト値 2-2, 2-3
アクセス
クライアントホスト 29-10

パーティション 23-5
アクセス権限
VLAN の作成 21-5, 28-4, 28-5, 28-7, 28-10
スタティックルートの追加 21-9
セルフ IP アドレスの作成 21-6, 21-7, 21-8
特定 23-1
ユーザアクセスも参照
アクセス制御
設定 24-7
調整 23-1
アクセス制御グループ
パーティションを参照
アクセス制御の組み合わせ 24-8
アクセス制御プロセス
承認手順を参照
アクセス制御プロパティ
設定 24-6
アクセス要求パケット 25-8
アクセスレベル
Common パーティション 23-2
ユーザアクセスも参照
アグリゲーション、リンク 17-1
アダプティブコネクションリーパ 22-2, 22-3
圧縮
iRule 10-1
RAM キャッシュ 13-1
WAN 上 28-1
オフにする 28-2
設定 12-4
ダイナミックに生成されたデータ 28-2
圧縮作業 10-1
圧縮の統計情報
トンネリング 28-12
圧縮方式
定義 28-2
宛先アドレス変換 2-1
アドレス変換 2-1, 2-2, 7-5
アプリケーション
高速化ポリシー 29-7
アプリケーションセキュリティ
有効化 29-4
アプリケーションプロファイル
WebAccelerator 29-7
作成 30-1
セキュリティポリシーへの割り当て 29-12
設定 29-9, 30-9
定義 29-7, 30-7
ホストマップ 29-8, 30-8
アプリケーションプロファイルの検証 30-10
暗号化
トンネリング 28-1
アンマップドメイン
アンマップドメインを参照

い

一般的な設定 6-1
インターネット接続
追加 7-1
例 7-1
ロードバランシング 7-1
インターフェイス
使用、リンクアグリゲーション 17-1
パーティション 23-2
割り当て、タグ付きとして 5-2
イントラネット設定 6-1
作成 6-2

え

エンドポイントプール 28-10
作成 28-4

お

応答
圧縮 10-1
暗号化 11-1, 12-1
応答タイプ 13-1
オブジェクト
Guest ロール 23-3
需要 13-1
定義 23-1
表示と管理 23-4
オブジェクトの再利用 13-1
オブジェクトの作成
パーティションの場所 23-5
オンラインヘルプ 1-5

か

カスタマ
ホスティング 5-1
カスタム HTTP プロファイル
使用 8-1
カスタム RADIUS プロファイル
割り当て 25-9
カスタムパーシステンスプロファイル
使用 8-1
説明 9-1
カスタムモニタ 19-1
仮想認証サーバ
VLAN 27-2
定義 27-1
管理ドメイン
定義 23-1
管理パーティション
トンネリング 28-3

き

キーのインストール 12-1
企業イントラネット 6-1
キャッシュサーバ 6-1
キャッシュ指示 29-7, 29-8

く

クライアントの資格情報 25-7
クライアントホスト
アプリケーションアクセス 30-10
クライアント要求
BIG-IP 2-6
復号化 11-6

グループ
　特権の割り当て 24-7
　ユーザアクセス制御 24-1
クロック同期

け

継承の防止
　モニタ 19-5
ゲートウェイ
　nPath ルーティング 2-5

こ

広域ネットワーク
　トラフィックの最適化 28-1
高需要オブジェクト 13-1
構成例、インターネット 3-1
高速化
　トラフィックへの適用 29-3
　有効化 29-4
高速化ポリシー 29-8
　Level 1 Delivery 29-7, 30-7
　Level2 Delivery 29-7
　WebAccelerator 30-10
　署名付きの高速化ポリシー 29-8, 30-8
　対向設置 30-8
　ユーザ定義の高速化ポリシー 29-8, 30-8
　レベル 2 配信 30-7
コネクションリーパ 22-9
コマンドラインインターフェイス
　bigpipe シェルを参照
コンテンツ
　需要 13-1
　スタティック 13-1
コンテンツ圧縮
　RAM キャッシュ 13-1
コンテンツ要求 29-7

さ

サーバ SSL プロファイル
　トンネリング 28-6
サーバ応答
　暗号化 11-1, 11-6, 12-1
サーバのホスティング 3-1
サーバプール
　nPath ルーティング 2-4
サーバ負荷 13-1
サービス拒否攻撃 22-1, 22-8
サービス拒否攻撃の防御 22-4
サービスポート
　トンネリング 28-11
サービスポート 3701 28-11
最高点
　アダプティブコネクションリーパを参照
再送信タイムアウト
　RTO を参照
最低点
　アダプティブコネクションリーパを参照
サブドメイン
　マッピング 29-8

し

式
　パケットフィルタリング 18-1
自己署名証明書 11-2, 12-2
システムアクセス
　制御 23-1
システムオブジェクト
　表示と管理 23-4
システムリソース消費 22-8
事前定義済みの高速化ポリシー
　Level 1 Delivery 30-7
　選択 29-7, 30-7
　レベル 1 配信 29-7
　レベル 2 配信 29-7, 30-7
状態の保持 22-8
承認失敗 24-9
承認手順 23-2
承認プロパティ
　設定 24-6
承認レベル
　特定 23-3
証明書のインストール 12-1
書式規則 1-3
署名付きの高速化ポリシー
　定義 29-8, 30-8
シンプルパーシステンス 8-1

す

数値
　ユーザ特権 24-9
スタティックコンテンツ 13-1
スマーフ攻撃 22-9
スループット
　増加 2-1
スループットの最適化 16-5

せ

正規表現 10-1
脆弱性
　スキャン 30-4
セカンダリ RADIUS サーバ
　設定 24-4
セキュリティ
　トラフィックへの適用 29-3
セキュリティチェック
　HTTP セキュリティプロファイル 30-12
　HTTP トラフィック 30-5
セキュリティポリシー
　アプリケーションプロファイル 29-12
セッションパーシステンス
　Cookie パーシステンスも参照
　実装 8-1
　送信元アドレスのアフィニティパーシステンスも参照
接続
　インターネット接続も参照
　追加 7-1
　認証 25-7
　リープ 22-2
接続タイムアウト 2-6, 22-8

接続フラッド 22-9
接続要求タイプ 6-1
設定済みモニタ 19-1
設定データ
インポートとエクスポート 24-11
設定ユーティリティ
Welcome 画面 1-5
オンラインヘルプ 1-5
設定用ワークシート 1-2
セルフ IP アドレス
外部 VLAN 7-5
削除 4-3, 17-7
作成 17-8
作成、VLAN グループ 4-5
パーティション 23-2

そ

送信スループット
増加 2-1
送信元 IP アドレス
セッションパーシステンス 8-2
送信元アドレスのアフィニティパーシステンス 8-1
送信元アドレス変換 2-1

た

ターミナルアクセスプロパティ 24-6
対向設置高速化ポリシー 30-8
対称展開
コンテンツアセンブリ 29-10
定義 29-8
タイマ 2-6
タグ付きインターフェイス 5-2, 17-1
単一設定ファイル
SCF を参照
アクセス制御 24-1

ち

着信トラフィック 7-3
重複する IP アドレス 21-1
割り当て 21-1

て

データ圧縮
RAM キャッシュ 13-1
WAN 上 28-1
データ圧縮の統計情報
トンネリング 28-12
データ暗号化
トンネリング 28-1
データ検証
WebAccelerator 29-10, 30-10
データ攻撃 22-11
データ最適化
トンネリング 28-1
データセンターのトポロジ 4-1
データタイプ
トンネリング 28-2
データ伝播 24-7, 24-11
デフォルト HTTP プロファイル
使用 8-1
デフォルトのパーシステンスプロファイル
使用 8-1
説明 9-1
デフォルトルート
nPath ルーティング 2-2
設定 2-2, 16-4
デフォルトワイルドカードサーバ 6-1
展開シナリオ
定義 29-13
電子商取引トラフィック
ロードバランシング 3-1
転送バーチャルサーバ
トンネリング 28-9

と

特権
アクセス制御も参照
個別アカウント 24-6
設定 24-6
割り当て 24-7
トポロジ 4-1
ドメイン
特定 29-8
ドメインの検証とマッピング 29-11
トラフィック
同じネットワーク 4-4
戻り 2-1
トラフィック負荷 13-1
トランク 17-3
トランクメンバ 17-3
トンネリング
エンドポイントプールも参照 28-4
データ最適化 28-1
トンネリングも参照

な

内蔵スイッチング
複数カスタマのホスティング 5-5
名前解決
設定 30-2

に

認証サーバ
プールメンバとして 27-1
認証サーバのタイプ 24-2
認証属性 24-9, 24-10
認証データ
伝播 24-1
認証モジュールの種別 25-7

ね

ネットマスク 2-4
ネットワーク
変更 4-1
ネットワークアダプタリスト 2-5
ネットワーク設定
IP ネットワークトポロジ 16-1

リンクアグリゲーション 17-2, 17-6
ネットワークトラフィック
管理 2-1
追加接続 7-1
パケットフィルタ 18-1
ネットワークトラフィック認証のタイプ 25-1
ネットワークプレフィックス 20-1

の

ノード
Operator ロール 23-3
ルートドメイン 21-1
ノード設定
radvd サービス 20-1

は

パーシステンス 2-6
Cookie パーシステンスも参照
実装 8-1
パーシステンスプロファイル
作成 9-2
割り当て、FTP 14-4
割り当て、HTTP 9-4
割り当て、HTTPS 11-6
割り当て、RAM キャッシュ 13-3
割り当て、圧縮 12-7
バーチャルサーバ
FTP 14-4
FTP とレートシェイピング 15-5
HTTP 8-3
HTTPS 11-6, 12-7
HTTP クラスプロファイル 29-4
IPv6 ノード 20-3
iSession エンドポイント 28-10
nPath ルーティング 2-4
RAM キャッシュ 13-3
SNAT 16-1
Web サーバプール 4-6
圧縮 10-3
基本設定 6-3, 18-3
作成、HTTP 用 9-4
作成、イントラネット設定 6-3
作成、単一ネットワーク 16-3
作成、着信トラフィックと発信トラフィック 7-3
作成、電子商取引 3-3
作成、複数カスタマのホスティング 5-3
設定 29-5
電子商取引 3-1
トンネリング 28-6
複数カスタマのホスティング 5-3
変更、CRLDP 認証 25-22
変更、RADIUS 認証 25-10
変更、SSL OCSP 認証 25-19
変更、SSL クライアント証明書 LDAP 認証 25-16
変更、TACACS+ 認証 25-13
マッピング、IP アドレス 2-4
リンクアグリゲーション 17-5
バーチャルサーバアドレス 2-2
バーチャルサーバの変更 25-10
バーチャルサーバ
定義 30-5
パーティション
作成 23-2
選択 23-5
定義 23-1
トンネリング 28-3
ユーザロール 23-2
利点 23-2
パーティションアクセス
設定 23-3
パーティションアクセスリスト 23-4
パーティションコンテンツ 23-1
パーティションプロパティ 24-6
パーティション分割オブジェクト
作成 23-5
説明 23-2
パケット
受信とコピー 4-4
認識、クライアント 16-5
フォワーディングと拒否 18-1
パケットフィルタ 18-1, 18-4
パケットフィルタルール
作成 18-4
目的 18-1
パスワード資格情報 25-7
パフォーマンスモニタ 19-2
汎用事前定義済み高速化ポリシー 29-7

ひ

表記規則 1-3
標準の事前定義済み高速化ポリシー 30-7

ふ

ファイル
包含と除外 10-1
プール
HTTP クラスプロファイル 29-4
Web サーバ 4-5
作成、FTP サーバ 14-3
作成、HTTPS 11-5, 12-6
作成、HTTP 用 8-2, 9-3
作成、ISP のロードバランシング 7-2
作成、nPath ルーティング 2-4
作成、イントラネット設定 6-2
作成、基本設定 6-2
作成、単一ネットワーク 16-2
作成、電子商取引 3-1, 3-2
作成、複数カスタマのホスティング 5-3
作成、モニタ 19-4
作成、ルータ 18-2
作成、レートシェイピング 15-3
設定 29-5
リンクアグリゲーションの作成 17-4
プールメンバ
Operator ロール 23-3
トンネルエンドポイント 28-10
ルートドメイン 21-1
プールメンバの除外 19-4, 19-5

複数カスタマのホスティング
概要 5-1
作成、VLAN タグ 5-2
作成、プール 5-3
設定 5-2
内蔵スイッチングの使用 5-5
フラッド 22-9
ブロードキャストアドレス 2-4
プロトコル
リモート認証サーバ 25-1
プロトコルセキュリティチェック 30-5
プロトコルセキュリティモジュール
WebAccelerator とともに実行 30-3
セキュリティプロファイル 30-1
プロトコルの脆弱性
スキャン 30-4
プロビジョニング
モジュール 30-2
プロファイル
作成、HTTP 用 10-2, 25-15
プロファイルの検証 30-10

へ

ペアトンネリング 28-1
定義 28-1
ヘルスモニタ
リモート認証サーバ 27-1
ヘルプ、オンライン 1-5
変数置換
アクセス制御 24-8
ベンダ固有の属性 24-7, 24-8

ほ

ポート
電子商取引用 3-1
ポート透過性
定義 28-11
ポート変換 2-2
ホストマップ
要求ホスト 29-8, 30-8
ホストマップの検証 29-11
ホスト名
指定 29-8
補足情報
Bigpipe Utility Reference Guide 1-2
『Configuration Guide for BIG-IP Local Traffic Management』 1-2
Installation, Licensing, and Upgrades for BIG-IP Systems 1-2
Platform Guide 1-2
TMOS Management Guide for BIG-IP Systems 1-2
設定用ワークシート 1-2

も

モニタ
削除 19-5
作成 19-3
作成、FTP サーバ 14-2, 15-2
定義 19-1
割り当て、プール 19-4
モニタタイプ 19-1
モニタの継承 19-4
モニタの設定 19-1

ゆ

ユーザアカウント
定義 23-1
ユーザアカウントオブジェクト
Manager ロール 23-3
ユーザアカウント複製 24-7
ユーザアカウントプロパティ
変更 23-3
ユーザアクセス
Common パーティション 23-2
拒否 24-8
設定 23-3
調整 23-1
ユーザ定義の高速化ポリシー
説明 29-8, 30-8
ユーザ特権
割り当て 24-7
ユーザ認証
設定 24-1
ユーザパーティションプロパティ 24-6
ユーザ名資格情報 25-7
ユーザロール
Create ボタン 21-5, 21-6, 21-7, 21-8, 21-9, 28-4, 28-5, 28-7, 28-10
定義 23-1
トンネリング 28-3
パーティションアクセス 23-2
パーティション作成 23-2
ユーザロールプロパティ 24-6
ユニバーサルアクセス 23-5

よ

要求
暗号化 11-1, 12-1
復号化 11-1, 12-1
要求タイムアウト 29-11
要求ホスト
定義 29-8
ドメイン 29-8, 30-8

り

リソース消費 22-8
リモート属性マッピング 24-7
リモート認証
システムユーザアカウント 24-2
リモート認証サーバのタイプ 24-2, 25-1
リモート認証属性 24-9, 24-10
リモート認証の条件 27-2
リモート認証の問題点 27-1
リモートポリシー 29-10
リモートユーザ認証
設定 24-1
リンクアグリゲーション
VLAN グループ 17-7

概要 17-1
設定 17-2
ネットワーク構成 17-6

る

ルータ
増加、スループット 2-1
ルータプール 18-2
ルーティング衝突 4-5
ルーティングテーブル
ルートドメイン 21-1
ルート
nPath ルーティング 2-5
パケット 4-5
ルート設定
nPath ルーティング 2-2
ルートドメイン
定義 21-1
トンネリング 28-3
ルートドメイン ID
フォーマット 21-1
ループバックインターフェイス 2-2, 2-5

れ

レートクラス
作成 15-4
バーチャルサーバ 15-5
レートシェイピング
FTP トラフィック 15-4
オプション機能 15-1
レベル 2 配信高速化ポリシー 30-7

ろ

ローカルエンドポイント 28-8, 28-11
ロール
トンネリング 28-3
ロールプロパティ 24-6

わ

ワイルドカードバーチャルサーバ
定義 6-1